PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-052029
(43)Date of publication of application : 21.02.2003

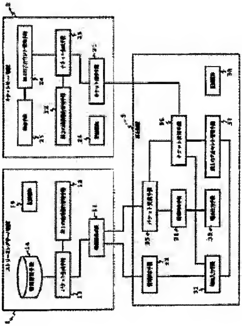
(51)Int.Cl. H04N 7/16
G06F 17/60
H04L 9/08
H04L 9/32
H04N 7/167
H04N 7/173

(21)Application number : 2001-237326
(22)Date of filing : 06.08.2001

(71)Applicant : NEC CORP
(72)Inventor : NAKAE MASAYUKI

(54) INFORMATION PROVIDING DEVICE, TICKET PROVIDING DEVICE, REPRODUCING DEVICE AND INFORMATION SELLING METHOD AND ITS PROGRAM

(57)Abstract:



PROBLEM TO BE SOLVED: To provide an information selling system for allowing the sales person of information to freely set the selling condition of information owned by the sales person himself or herself, in an information selling configuration that the sales person of information is different from the operator of a streaming system.

SOLUTION: This streaming system is provided with a streaming server device 1 to be managed by the operator of this system, a ticket server device 2 to be managed by the sales person of information, and a reproducing device 3 to be used by a user. The streaming server device 1 and the ticket server device 2 are respectively provided with a first transmission terms of agreement managing means 12, and a second transmission convention managing means 22 for individually managing a transmission terms of agreement prepared based on the consignment contract of the information distribution processing preliminarily concluded between the sales person of the information and the operator of the streaming system.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開2003－52029

（P2003－52029A）

(43)公開日　平成15年2月21日(2003.2.21)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード*(参考)
Ｈ０４Ｎ　7/16		Ｈ０４Ｎ　7/16	Ｃ　５Ｃ０６４
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ　５Ｊ１０４
	３３２		３３２
	５１２		５１２
	ＺＥＣ		ＺＥＣ

審査請求　有　請求項の数32　ＯＬ　（全 31 頁）　最終頁に続く

(21)出願番号　特願2001－237326(P2001－237326)

(22)出願日　平成13年8月6日(2001.8.6)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72)発明者　中江　政行
東京都港区芝五丁目7番1号　日本電気株式会社内

(74)代理人　100088812
弁理士　▲柳▼川　信

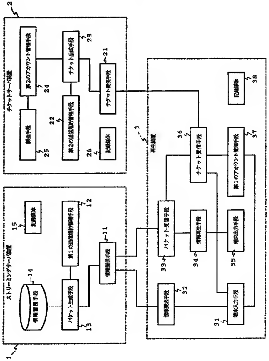
最終頁に続く

(54)【発明の名称】　情報提供装置、チケット提供装置、再生装置及びそれに用いる情報販売方法並びにそのプログラム

(57)【要約】

【課題】　情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、情報の販売者が自己の所有する情報の販売条件を自由に設定可能な情報販売システムを提供する。

【解決手段】　ストリーミングシステムの運用者が管理するストリーミングサーバ装置１と、情報の販売者が管理するチケットサーバ装置２と、利用者が使用する再生装置３とを備えるシステムにおいて、予め情報の販売者とストリーミングシステム運用者との間で結ばれた情報配信処理の委託契約に基づいて作成された送信規約を個別に管理するための第１の送信規約管理手段１２及び第２の送信規約管理手段２２をそれぞれストリーミングサーバ装置１及びチケットサーバ装置２に備えている。



【特許請求の範囲】

【請求項１】　情報をユーザに提供する情報提供装置であって、前記情報を暗号化するための情報暗号鍵と前記ユーザに対する販売条件とを少なくとも含む第１の送信規約を管理する第１の送信規約管理手段と、前記ユーザからの情報要求時に前記情報暗号鍵を用いて暗号化した情報を単に前記ユーザに送信する情報提供手段とを有することを特徴とする情報提供装置。

【請求項２】　前記ユーザからの情報要求時にその情報要求メッセージを受信する度に当該メッセージの送信元と通信しながら前記情報暗号鍵を変形するための情報を示すセッション鍵を確立するセッション鍵確立手段と、前記情報暗号鍵を当該セッション鍵を用いて変形させた鍵によって前記情報を暗号化する第２のパケット生成手段とを含むことを特徴とする請求項１記載の情報提供装置。

【請求項３】　前記情報は、その受信と再生とが並列的に行われるストリーミングデータであることを特徴とする請求項１または請求項２記載の情報提供装置。

【請求項４】　ユーザに対する情報提供時に前記ユーザに対する認証処理と課金処理とを行うチケット提供装置であって、暗号化された情報を復号して再生可能とするための情報復号鍵と前記ユーザに対する販売条件とを少なくとも含む第２の送信規約を管理する第２の送信規約管理手段を有することを特徴とするチケット提供装置。

【請求項５】　情報をユーザに販売するにあたって予め蓄積された当該ユーザの利用者情報及び当該ユーザの使用装置情報を含むクライアント情報と前記第２の送信規約とを基に当該ユーザの認証処理を行う第２のアカウント管理手段と、前記第２の送信規約を基に前記ユーザに対する課金処理を行う課金手段とを含むことを特徴とする請求項４記載のチケット提供装置。

【請求項６】　前記第２の送信規約の有無と、前記第２の送信規約に記載されかつ少なくとも有効期間を含む有効性に関する条件と、前記ユーザのクライアント情報の正当性とをそれぞれ判定してそれらのいずれかが無効と判定した時に前記ユーザに対して前記情報復号鍵を含むチケットの発行を抑止するチケット生成手段を含むことを特徴とする請求項５記載のチケット提供装置。

【請求項７】　前記第２の送信規約を管理する複数の第２の送信規約管理手段と、前記チケットの要求時にその要求内容に応じて前記複数の第２の送信規約管理手段のうちのいずれかを選択する送信規約グループ管理手段とを含むことを特徴とする請求項６記載のチケット提供装置。

【請求項８】　前記情報は、その受信と再生とが並列的に行われるストリーミングデータであることを特徴とする請求項４から請求項７のいずれか記載のチケット提供装置。

【請求項９】　情報提供装置から提供されかつ情報を暗号化するための情報暗号鍵を用いて暗号化された情報を、チケット提供装置から提供されかつ前記暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットに基づいて復号しつつ再生可能とするパケット受信手段を有することを特徴とする再生装置。

【請求項１０】　前記情報提供装置から前記情報暗号鍵を変形するための情報を示すセッション鍵が送られてきた時にそのセッション鍵を用いて前記セッション鍵で変形された鍵を生成する手段と、その生成された鍵を用いて前記セッション鍵で変形させた鍵によって暗号化された情報を復号する第２のパケット受信手段とを含むことを特徴とする請求項９記載の再生装置。

【請求項１１】　前記情報は、その受信と再生とが並列的に行われるストリーミングデータであることを特徴とする請求項９または請求項１０記載の再生装置。

【請求項１２】　情報を暗号化してユーザに提供するための情報暗号鍵と前記ユーザに対する販売条件とを少なくとも含む第１の送信規約を基に前記情報を暗号化するステップと、その暗号化した情報を前記ユーザからの情報要求時に当該ユーザに送信するステップとを前記情報を提供する情報提供装置に有し、

前記暗号化された情報を復号して再生可能とするための情報復号鍵と前記ユーザに対する販売条件とを少なくとも含む第２の送信規約を基に前記情報の販売時に前記情報復号鍵を含むチケットの発行を行うステップを前記チケットを提供するチケット提供装置に有することを特徴とする情報販売方法。

【請求項１３】　前記情報の販売時に予め蓄積された前記ユーザの利用者情報及び当該ユーザの使用装置情報を含むクライアント情報と前記第２の送信規約とを基に当該ユーザの認証処理を行うステップと、前記第２の送信規約を基に前記ユーザに対する課金処理を行うステップとを前記チケット提供装置に含み、

要求された情報を前記ユーザに送信するにあたって前記情報提供装置が前記暗号化された情報の送出を単に行うようにしたことを特徴とする請求項１２記載の情報販売方法。

【請求項１４】　前記第２の送信規約の有無と、前記第２の送信規約に記載されかつ少なくとも有効期間を含む有効性に関する条件と、前記ユーザのクライアント情報の正当性とをそれぞれ判定してそれらのいずれかが無効と判定した時に前記チケット提供装置が前記ユーザに対して前記チケットの発行を抑止するようにしたことを特徴とする請求項１３記載の情報販売方法。

【請求項１５】　前記チケット提供装置は、前記チケットを要求するメッセージの内容に応じて前記第２の送信規約を管理する複数の第２の送信規約管理手段のうちのいずれかを選択するようにしたことを特徴とする請求項１２から請求項１４のいずれか記載の情報販売方法。

【請求項１６】　前記チケットを要求するメッセージを前記チケット提供装置に送信するステップと、前記メッセージに応答して適切な情報復号鍵を含むチケットを得た時に当該チケットを基に前記情報提供装置で暗号化された情報を復号しつつ再生可能とするステップを前記情報を再生使用する再生装置に含むことを特徴とする請求項１２から請求項１５のいずれか記載の情報販売方法。

【請求項１７】　前記情報を要求するメッセージを受信する度に当該メッセージの送信元である前記再生装置と通信しながら前記情報暗号鍵を変形するための情報を示すセッション鍵を確立するステップと、前記情報暗号鍵を当該セッション鍵を用いて変形させた鍵によって前記情報を暗号化するステップとを前記情報提供装置に含み、

前記情報提供装置から前記セッション鍵が送られてきた時にそのセッション鍵を用いて前記セッション鍵で変形された鍵を生成するステップと、その生成された鍵を用いて前記セッション鍵で変形させた鍵によって暗号化された情報を復号するステップとを前記再生装置に含むことを特徴とする請求項１６記載の情報販売方法。

【請求項１８】　前記情報提供装置は、販売対象となる情報と当該情報に対応する前記第１の送信規約とを管理し、

前記チケット提供装置は、前記情報に対応する前記第２の送信規約を管理するようにしたことを特徴とする請求項１２から請求項１７のいずれか記載の情報販売方法。

【請求項１９】　前記チケット提供装置は、前記情報の代金をユーザから徴収した時に前記チケットを前記ユーザに提供するとともに、前記情報の代金の徴収時に前記情報提供装置の運用者に対して所定の委託契約に基づいた配信手数料を支払うようにしたことを特徴とする請求項１２から請求項１８のいずれか記載の情報販売方法。

【請求項２０】　前記情報提供装置が前記暗号化された情報の提供を専ら行い、前記チケット提供装置が前記販売条件にしたがった適切な課金及び正当と認められるユーザに対する前記チケットの提供を行うようにしたことを特徴とする請求項１２から請求項１９のいずれか記載の情報販売方法。

【請求項２１】　前記販売条件の変更及び前記情報の販売停止を行う時に、前記チケット提供装置で前記第２の送信規約の変更及び破棄を行うようにしたことを特徴とする請求項１２から請求項２０のいずれか記載の情報販売方法。

【請求項２２】　前記情報の配信に係る委託を複数の情報提供装置の運用者に対して行う時に前記チケット提供装置の運用者と前記情報提供装置の運用者との間で個別に締結された委託契約に基づいて作成される販売条件の組を前記チケット再生装置に登録し、前記販売条件に対応する前記第１の送信規約を前記情報提供装置で管理し、前記販売条件に対応する前記第２の送信規約を前記チケット提供装置で管理するようにしたことを特徴とする請求項１２から請求項２１のいずれか記載の情報販売方法。

【請求項２３】　前記再生装置の利用者が前記暗号化された情報の提供を受ける際に、前記再生装置から前記チケット提供装置に当該利用者の識別や課金に必要な情報を送信し、前記再生装置が前記チケット提供装置から前記チケットを取得して前記暗号化された情報を復号しながら再生するようにしたことを特徴とする請求項１２から請求項２２のいずれか記載の情報販売方法。

【請求項２４】　前記情報は、その受信と再生とが並列的に行われるストリーミングデータであることを特徴とする請求項１２から請求項２３のいずれか記載の情報販売方法。

【請求項２５】　コンピュータに、暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットを要求するメッセージを受信する処理と、その受信したメッセージから前記情報を識別するための情報識別子を抽出する処理と、この抽出された情報識別子を基に前記情報復号鍵とユーザに対する販売条件とを少なくとも含む複数の第２の送信規約のうちのいずれかを選択する処理と、前記メッセージの正当性を確認する処理と、選択された第２の送信規約に記載された課金額分の課金を行う処理と、選択された第２の送信規約を基に前記チケットを生成する処理とを実行させるためのプログラム。

【請求項２６】　前記コンピュータに、受信したメッセージから運用者識別子及び前記情報識別子からなる識別子を抽出する処理と、抽出した識別子を前記運用者識別子及び前記情報識別子に分割する処理と、分割された運用者識別子に対応する第２の送信規約の集合を選択する処理と、選択した第２の送信規約の集合の中から前記情報識別子に対応する送信規約を選択する処理とをさらに実行させることを特徴とする請求項２５記載のプログラム。

【請求項２７】　コンピュータに、情報を要求するメッセージを受信する処理と、その受信したメッセージから前記情報を識別するための情報識別子を抽出する処理と、抽出した情報識別子を基に前記情報を暗号化するための情報暗号鍵とユーザに対する販売条件とを少なくとも含む複数の第１の送信規約のいずれかと当該情報とを選択する処理と、前記第１の送信規約に記載された情報暗号鍵によって前記情報を読込みながら暗号化を行う処理とを実行させるためのプログラム。

【請求項２８】　前記コンピュータに、前記情報暗号鍵を変形するための情報を示すセッション鍵をランダムに生成して送信する処理と、前記情報暗号鍵を前記セッション鍵で変形させた鍵を生成して保持する処理とをさらに実行させることを特徴とする請求項２７記載のプログラム。

【請求項２９】　前記コンピュータに、前記情報暗号鍵を変形するための情報を示すセッション鍵を要求しかつ予め設定された第１のセッション鍵を含むメッセージを受信した後に当該メッセージから前記第１のセッション鍵を抽出する処理と、第２のセッション鍵をランダムに生成して送信する処理と、前記第１のセッション鍵と前記第２のセッション鍵とを関数にかけた値を用いて情報復号鍵を変形させた鍵を生成して保持する処理とをさらに実行させることを特徴とする請求項２８記載のプログラム。

【請求項３０】　コンピュータに、暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットを要求するメッセージを生成して送信する処理と、前記チケットを受信する処理と、受信したチケットから前記情報復号鍵を抽出して保持する処理と、その抽出した情報復号鍵を用いて受信した情報を復号しながら再生する処理とを実行させるためのプログラム。

【請求項３１】　前記コンピュータに、前記情報暗号鍵を変形するための情報を示すセッション鍵を受信する処理と、前記情報復号鍵を前記セッション鍵で変形させた鍵を生成して保持する処理とをさらに実行させることを特徴とする請求項３０記載のプログラム。

【請求項３２】　前記コンピュータに、前記情報暗号鍵を変形するための第１のセッション鍵をランダムに生成して保持する処理と、前記第１のセッション鍵を含むセッション鍵を要求するメッセージを送信する処理と、第２のセッション鍵を受信した後に前記第１のセッション鍵と前記第２のセッション鍵とを関数にかけた値を用いて前記情報復号鍵を変形させた鍵を生成して保持する処理とをさらに実行させることを特徴とする請求項３０記載のプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は情報提供装置、チケット提供装置、再生装置及びそれに用いる情報販売方法並びにそのプログラムに関し、特に提供する利用者の性質や時刻等を基にした多様な課金制御を行う情報販売システムに関する。

【０００２】

【従来の技術】従来、インタネットを利用したビデオ／音楽等の情報提供方法としては、情報をいくつかの通信パケットに断片化し、各通信パケットを順次送受信しつつ、情報を再生していくような「ストリーミング方式」が一般に知られている。以下、ストリーミング方式を利用した情報提供システムを「ストリーミングシステム」と呼ぶ。

【０００３】このようなストリーミングシステムを用いて情報を販売する方法は既に知られており、それを利用した情報販売システムの一例として、特開２００１－４３４４０号公報に開示されたシステムや、特開２０００－１２４９００号公報に開示されたシステム等がある。これらのシステムはいずれも、ストリーミングシステム内に課金手段を用意している。したがって、ストリーミングシステムは情報提供処理に加えて、課金に係るユーザ認証処理や課金処理等を同一システム内で行うものである。

【０００４】また、一般の情報販売システムにおいて、情報の送出処理を専ら行う情報提供システムの外に、ユーザ認証処理や課金処理等を専ら行う課金システムを備えるような情報販売システムも知られており、それらについての一例が、特開平１１－９８１３６号公報や特開平１０－１２４５７６号公報等に記載されている。

【０００５】特開平１１－９８１３６号公報記載の情報販売システムでは、情報提供システム（「データ提供者のサーバ」）の外に、課金システム（「中継サーバ」）が備えられており、課金システムは、一般によく知られた「プロキシ」として動作する。

【０００６】情報販売システムにおいては、ユーザから情報提供システムへ情報提供を要求するにあたり、課金システムを必ず経由する必要があり、さらに課金システム上でユーザ認証処理や課金処理が行われ、その後、情報提供システムから送出された情報が課金システムを経由してユーザへ伝達される。この場合、課金システムはユーザ認証処理や課金処理に加えて、情報提供処理をも併せて行うことになり、この点において、上記のようなストリーミングシステムと同等といえる。

【０００７】一方、特開平１０－１２４５７６号公報記載の情報販売システムでは、「情報提供装置」及び「鍵管理装置」から構成される情報提供システムと、「情報管理装置」から構成される課金システムとを備えている。

【０００８】ユーザから情報提供システムへ情報提供を要求すると、情報提供システムの情報提供装置から暗号化された情報が送出され、加えて鍵管理装置から暗号化情報の復号鍵が送出される。ここで、各ユーザの利用する端末と、情報提供システムを構成する２つの装置とにはそれぞれ、「回線接続装置」が備えられており、課金システムはこれら回線接続装置の識別及び回線接続装置間の通信記録を蓄積することができる。

【０００９】したがって、課金システムはユーザ及び情報提供システムとの間で交わされる情報提供処理に関するすべての記録を基に、適切な課金処理を行うことができる。しかしながら、課金システムはユーザ及び情報提供システム間の通信を遮断することはできないので、支払い能力の有無やユーザの識別情報の正当性等を検査し、必要に応じて情報提供処理を中断する等といったユーザ認証処理を行うことができない。

【００１０】また、一般に、インタネット上の情報販売システムにおいては、ユーザ及び情報提供システム間の通信内容が、例えばＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅ

ｔＬａｙｅｒ）等の暗号化通信方式によって暗号化されている場合が多く見られるが、このような場合に、課金システムでは適切な課金処理を行うことができない。

【００１１】

【発明が解決しようとする課題】上述した従来のストリーミングシステムでは、そのシステム上に課金サブシステムや利用者管理サブシステムを構築するため、販売者が価格の操作を行いたい場合や独自の利用者データベースを構築したい場合に、ストリーミングシステム運用者に上記のような各種サブシステムの再設定を依頼しなければならない上に、ストリーミングシステム運用者から見れば委託を受けているあらゆる販売者からの上記のような依頼に応えるのは実務上困難である。

【００１２】そのため、情報の販売者が自己の所有する情報の販売にあたって、外部のストリーミングシステム運用者に情報提供業務を委託するような場合、販売者自身が価格を自由に操作したり、販売者独自の顧客管理を行うことが困難であるという問題がある。

【００１３】また、ストリーミングシステムの持つ計算機資源及び通信資源は有限であり、かつ同システム上で利用者認証処理や課金処理を行うと各資源が余計に消費されるので、情報の送信処理に必要な各資源が圧迫される。そのため、ストリーミングシステム上で利用者認証処理や課金処理を行う場合、ストリーミングシステムが行う送信処理のパフォーマンスを低下させるという問題がある。

【００１４】さらに、従来のストリーミングシステムのように、ストリーミングシステム内で利用者認証処理や課金処理を行う場合には、利用者から得られる利益を正確に把握できるのがストリーミングシステム運用者のみであり、情報の販売者はストリーミングシステム運用者からの申告を信頼するよりほかない。

【００１５】そのため、上記の問題と同様に、情報の販売者とストリーミングシステムの運用者とが異なる場合には、情報提供の対価として利用者から得られる利益を、情報の販売者とストリーミングシステムの運用者とで分配する必要があるが、こうした利益分配が公正に行われる保証がないという問題がある。

【００１６】そこで、本発明の目的は上記の問題点を解消し、情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、情報の販売者が自己の所有する情報の販売条件（価格や利用者制限）を自由に設定することができる情報販売システム及び情報販売方法並びにそのプログラムを提供することにある。

【００１７】また、本発明の他の目的は、ストリーミングシステムが行う情報の送信処理のパフォーマンスを低下させることなく、利用者認証処理や課金処理を行うことができる情報販売システム及び情報販売方法並びにそのプログラムを提供することにある。

【００１８】さらに、本発明の別の目的は、情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、利用者から得られる利益を、情報の販売者とストリーミングシステムの運用者との間で公正に分配することができる情報提供装置、チケット提供装置、再生装置及びそれに用いる情報販売方法並びにそのプログラムを提供することにある。

【００１９】

【課題を解決するための手段】本発明による情報提供装置は、情報をユーザに提供する情報提供装置であって、前記情報を暗号化するための情報暗号鍵と前記ユーザに対する販売条件とを少なくとも含む第１の送信規約を管理する第１の送信規約管理手段と、前記ユーザからの情報要求時に前記情報暗号鍵を用いて暗号化した情報を単に前記ユーザに送信する情報提供手段とを備えている。

【００２０】本発明によるチケット提供装置は、ユーザに対する情報提供時に前記ユーザに対する認証処理と課金処理とを行うチケット提供装置であって、暗号化された情報を復号して再生可能とするための情報復号鍵と前記ユーザに対する販売条件とを少なくとも含む第２の送信規約を管理する第２の送信規約管理手段を備えている。

【００２１】本発明による再生装置は、情報提供装置から提供されかつ情報を暗号化するための情報暗号鍵を用いて暗号化された情報を、チケット提供装置から提供されかつ前記暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットに基づいて復号しつつ再生可能とするパケット受信手段を備えている。

【００２２】本発明による情報販売方法は、情報を暗号化してユーザに提供するための情報暗号鍵と前記ユーザに対する販売条件とを少なくとも含む第１の送信規約を基に前記情報を暗号化するステップと、その暗号化した情報を前記ユーザからの情報要求時に当該ユーザに送信するステップとを前記情報を提供する情報提供装置に備え、前記暗号化された情報を復号して再生可能とするための情報復号鍵と前記ユーザに対する販売条件とを少なくとも含む第２の送信規約を基に前記情報の販売時に前記情報復号鍵を含むチケットの発行を行うステップを前記チケットを提供するチケット提供装置に備えている。

【００２３】本発明による他の情報販売方法は、前記情報の販売時に予め蓄積された前記ユーザの利用者情報及び当該ユーザの使用装置情報を含むクライアント情報と前記第２の送信規約とを基に当該ユーザの認証処理を行うステップと、前記第２の送信規約を基に前記ユーザに対する課金処理を行うステップとを前記チケット提供装置に具備し、要求された情報を前記ユーザに送信するにあたって前記情報提供装置が前記暗号化された情報の送出を単に行うようにしている。

【００２４】本発明による別の情報販売方法は、前記チ

ケットを要求するメッセージを前記チケット提供装置に送信するステップと、前記メッセージに応答して適切な情報復号鍵を含むチケットを得た時にのみ当該チケットを基に前記情報提供装置で暗号化された情報を復号しつつ再生可能とするステップを前記情報を再生使用する再生装置に具備している。

【００２５】本発明による情報販売方法のプログラムは、コンピュータに、暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットを要求するメッセージを受信する処理と、その受信したメッセージから前記情報を識別するための情報識別子を抽出する処理と、この抽出された情報識別子を基に前記情報復号鍵とユーザに対する販売条件とを少なくとも含む複数の第２の送信規約のうちのいずれかを選択する処理と、前記メッセージの正当性を確認する処理と、選択された第２の送信規約に記載された課金額分の課金を行う処理と、選択された第２の送信規約を基に前記チケットを生成する処理とを実行させている。

【００２６】本発明による他の情報販売方法のプログラムは、コンピュータに、情報を要求するメッセージを受信する処理と、その受信したメッセージから前記情報を識別するための情報識別子を抽出する処理と、抽出した情報識別子を基に前記情報を暗号化するための情報暗号鍵とユーザに対する販売条件とを少なくとも含む複数の第１の送信規約のいずれかと当該情報とを選択する処理と、前記第１の送信規約に記載された情報暗号鍵によって前記情報を読込みながら暗号化を行う処理とを実行させている。

【００２７】本発明による別の情報販売方法のプログラムは、コンピュータに、暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットを要求するメッセージを生成して送信する処理と、前記チケットを受信する処理と、受信したチケットから前記情報復号鍵を抽出して保持する処理と、その抽出した情報復号鍵を用いて受信した情報を復号しながら再生する処理とを実行させている。

【００２８】すなわち、本発明の情報販売システムは、ストリーミングシステムの運用者が管理するストリーミングサーバ装置と、情報の販売者が管理するチケットサーバ装置と、利用者が使用する再生装置とを備え、ストリーミングサーバ装置に第１の送信規約管理手段を備え、チケットサーバ装置に第２の送信規約管理手段を備えることで、予め情報の販売者とストリーミングシステム運用者との間で結ばれた情報配信処理の委託契約に基づいて作成された送信規約を個別に管理するようにしている。

【００２９】また、第１の送信規約管理手段で保持される送信規約が情報暗号鍵を含むようにし、ストリーミングサーバ装置が再生装置に情報を提供する際に、パケット生成手段で、その情報を情報暗号鍵で暗号化したセキュアパケットを生成するようにしている。

【００３０】さらに、当該セキュアパケットを受信した再生装置は、チケット受信手段で予めチケットサーバ装置から、第２の送信規約管理手段で保持される送信規約に記載された情報復号鍵を含むチケットを受信するようにし、さらにパケット受信手段において、当該情報復号鍵によってセキュアパケットを復号するようにしている。

【００３１】さらにまた、チケットサーバ装置と再生装置との間で、上記のようなチケット通信を行う際には、再生装置のチケット受信手段及び第１のアカウント管理手段によって、ユーザから情報の販売者に情報の代金を支払うのに必要な決済用情報、もしくは決済用情報を特定するに十分なユーザＩＤ（識別情報）等のアカウンティング情報をチケット要求メッセージに含めるようにし、チケットサーバ装置の第２のアカウント管理手段で当該アカウンティング情報の正当性を確認するようにしている。

【００３２】加えて、チケット要求メッセージに情報識別子を含めるものとし、チケットサーバ装置の第２の送信規約管理手段から当該情報識別子に対応する送信規約を取得するようにし、送信規約に記載された課金額を課金手段に伝達するようにしている。

【００３３】上記のように、情報の販売者が自己の所有する情報の販売条件を送信規約として管理するためのチケットサーバ装置を備えることによって、情報の販売者がストリーミングシステムの運用者に情報の配信業務を委託する際に、情報の販売者が自己の所有する情報の販売条件を自由に設定することが可能となる。

【００３４】また、利用者認証処理や課金処理をストリーミングサーバ装置とは独立したチケットサーバ装置で行うことによって、情報の提供時にストリーミングシステムのパフォーマンスを低下させることなく、利用者認証処理や課金処理を安全に行うことが可能となる。

【００３５】さらに、情報の販売者とストリーミングシステムの運用者との間の合意に基づいてそれぞれの送信規約を作成し、それぞれが運用するチケットサーバ装置とストリーミングサーバ装置とで個別に管理することによって、情報の販売者とストリーミングシステムの運用者との間で公正な利益分配を行うことが可能となる。

【００３６】

【発明の実施の形態】次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例による情報販売システムの構成を示すブロック図である。図１において、本発明の一実施例による情報販売システムは情報を提供する情報提供装置であるストリーミングサーバ装置１と、チケットを提供するチケット提供装置であるチケットサーバ装置２と、提供された情報を再生する再生装置３とから構成されている。

【００３７】ストリーミングサーバ装置１は情報提供手

段１１と、第１の送信規約管理手段１２と、パケット生成手段１３と、情報蓄積手段１４と、各手段で実行されるプログラムを格納する記録媒体１５とから構成されている。

【００３８】情報提供手段１１は再生装置３から受信した情報提供要求メッセージ中に記載された情報識別子をパケット生成手段１３に伝達し、パケット生成手段１３から取得されるパケットあるいはエラーメッセージを再生装置３に送信する。

【００３９】第１の送信規約管理手段１２は１者以上の情報の販売者から与えられた全ての第１の送信規約を保持しており、パケット生成手段１３から情報識別子の入力を受けた時、それに対応する第１の送信規約に記載された情報暗号鍵をパケット生成手段１３に出力するか、あるいはエラーメッセージをパケット生成手段１３に出力する。ここで、第１の送信規約は提供する情報を暗号化するための情報暗号鍵とユーザに対する販売条件（送信タイミング、有効期間、課金条件等）とを少なくとも含んでいる。

【００４０】パケット生成手段１３は情報提供手段１１からユーザに提供すべき情報を識別するための情報識別子の入力を受けると、その情報識別子を第１の送信規約管理手段１２に入力し、その情報に対応する情報暗号鍵を取得するか、エラーメッセージを取得する。また、パケット生成手段１３はこの情報識別子を情報蓄積手段１４に入力し、ユーザに提供すべき情報を取得する。さらに、パケット生成手段１３はその情報とそれに対応する情報暗号鍵とから生成したセキュアパケットを順に情報提供手段１１に出力するか、あるいはエラーメッセージを情報提供手段１１に出力する。

【００４１】情報蓄積手段１４は１者以上の情報の販売者から与えられた全ての情報を保持しており、パケット生成手段１３から情報識別子の入力を受けた時、それに対応する情報をパケット生成手段１３に出力する。

【００４２】チケットサーバ装置２はチケット提供手段２１と、第２の送信規約管理手段２２と、チケット生成手段２３と、第２のアカウント管理手段２４と、課金手段２５と、各手段で実行されるプログラムを格納する記録媒体２６とから構成されている。

【００４３】チケット提供手段２１は再生装置３から受信したチケット要求メッセージをチケット生成手段２３に伝達し、チケット生成手段２３から取得したチケットを再生装置３に送信するか、あるいはエラーメッセージを再生装置３に送信する。ここで、チケットには再生装置３から要求される情報を復号して再生可能とするための情報復号鍵や上記の販売条件等を少なくとも含んでいる。

【００４４】第２の送信規約管理手段２２は１つ以上の第２の送信規約を保持しており、チケット生成手段２３からチケットが要求された情報を識別するための情報識別子の入力を受けると、それに対応する第２の送信規約をチケット生成手段２３に出力する。ここで、第２の送信規約には情報復号鍵と上記の販売条件とを少なくとも含んでいる。

【００４５】チケット生成手段２３はチケット提供手段２１からチケット要求メッセージの入力を受けると、そのチケット要求メッセージを第２の送信規約管理手段２２に伝達し、そのチケット要求メッセージに対応する第２の送信規約を取得する。また、チケット生成手段２３は当該チケット要求メッセージ内に記載されたクライアント情報及び第２の送信規約を第２のアカウント管理手段２４に伝達し、利用可否メッセージを取得する。さらに、チケット生成手段２３は生成したチケットチケット提供手段２１に出力するか、あるいはエラーメッセージをチケット提供手段２１に出力する。

【００４６】ここで、クライアント情報にはチケット要求メッセージを送ってきたユーザに対する認証処理や課金処理を行うために、ユーザを特定するための利用者情報やそのユーザが使用する端末装置を特定するための使用装置情報を含んでいる。

【００４７】第２のアカウント管理手段２４はチケットサーバ装置２でサポートするユーザもしくはホストに対する１つ以上のアカウントを保持しており、チケット生成手段２３からクライアント情報及び第２の送信規約の入力を受けた時、対応するアカウントの有無やその他の条件判定の結果等に応じて生成された利用可否メッセージをチケット生成手段２３に出力する。また、第２のアカウント管理手段２４は必要に応じて課金情報を課金手段２５に出力する。課金手段２５は第２のアカウント管理手段２４から課金情報の入力を受けると、適切な課金処理を行う。

【００４８】再生装置３は端末入力手段３１と、情報要求手段３２と、パケット受信手段３３と、情報再生手段３４と、端末出力手段３５と、チケット受信手段３６と、第１のアカウント管理手段３７と、各手段で実行されるプログラムを格納する記録媒体３８とから構成されている。

【００４９】端末入力手段３１はユーザからの入力を受けるためのキーボード装置や、マウス装置等の入力デバイスを備え、その入力デバイスからの入力データを適切に解釈し、チケット受信開始メッセージをチケット受信手段３６に出力する。また、端末入力手段３１は情報受信開始メッセージを情報要求手段３２に出力する。

【００５０】情報要求手段３２は端末入力手段３１から情報受信開始メッセージの入力を受けると、その情報受信開始メッセージ内に記載されたストリーミングサーバのＵＲＬ（Ｕｎｉｖｅｒｓａｌ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）等を基に適切なストリーミングサーバ装置１との間のコネクションを確立し、ストリーミングサーバ装置１に情報要求メッセージを送信する。

【００５１】パケット受信手段３３はストリーミングサーバ装置１からセキュアパケットを受信した際、チケット受信手段３６から入力された情報復号鍵を用いてそのセキュアパケットを復元した結果（復元パケット）を情報再生手段３４に出力する。情報再生手段３４はパケット受信手段３３から復元パケットの入力を受けると、適切な復元処理によって得られる再生データを端末出力手段３５に出力する。

【００５２】端末出力手段３５はユーザに情報を適切に提示するためのモニタ装置やスピーカ装置、及びミキサ装置等の出力デバイスを備えており、情報再生手段３４から再生データの入力を受けると、その再生データを出力デバイスに出力する。

【００５３】チケット受信手段３６は端末入力手段３１からチケット受信開始メッセージの入力を受けた際、第１のアカウント管理手段３６からクライアント情報を取得する。また、チケット受信手段３６はチケット受信開始メッセージ内に記載されたチケットサーバのＵＲＬを基に、適切なチケットサーバ装置２との間のコネクションを確立し、そのチケットサーバ装置２にチケット要求メッセージを送信する。

【００５４】第１のアカウント管理手段３７はユーザＩＤ（識別情報）やパスワード等の利用者情報を含むクライアント情報を保持しており、チケット受信手段３６からの要求に応じてクライアント情報をチケット受信手段３６に出力する。

【００５５】図２は本発明の一実施例による情報販売システムの動作を示すフローチャートであり、図３は図２のチケット要求処理を示すフローチャートであり、図４は図２のチケット要求確認処理を示すフローチャートである。

【００５６】図５は本発明の一実施例における送信規約管理表の一例を示す図であり、図６は本発明の一実施例における送信規約の一例を示す図であり、図７は本発明の一実施例におけるアカウント管理表の一例を示す図である。

【００５７】図８は図１のチケットサーバ装置２における決済センタへクライアント情報の正当性確認を委譲するための構成の一例を示す図であり、図９は図２の課金処理を示すフローチャートであり、図１０は図１のチケットサーバ装置２における決済センタを用いて課金処理を行うための構成の一例を示す図である。

【００５８】図１１は図２のチケット生成処理を示すフローチャートであり、図１２は本発明の一実施例におけるチケットのフォーマットの一例を示す図であり、図１３は図２のチケット受信処理を示すフローチャートであり、図１４は図２の情報要求処理を示すフローチャートである。

【００５９】図１５は図２の情報抽出処理を示すフローチャートであり、図１６は本発明の一実施例における情報管理表の一例を示す図であり、図１７は図２のパケット送出処理を示すフローチャートであり、図１８は図２の情報再生処理を示すフローチャートである。

【００６０】これら図１～図１８を参照して本発明の一実施例による情報販売システムの動作について説明する。尚、上記の図２～図４、図９、図１１、図１３～図１５、図１７、図１８に示す処理はストリーミングサーバ装置１、チケットサーバ装置２、再生装置３各々の各手段が記録媒体１５，２６，３８に夫々格納されたプログラムを実行することで実現される。

【００６１】本発明の一実施例による情報販売システムにおいて、まず、再生装置３はユーザ入力解釈処理を行う（図２ステップＡ３１）。具体的には、再生装置３の端末入力手段３１において、ユーザから情報識別子とストリーミングサーバ装置１の位置情報とチケットサーバ装置２の位置情報とに関する入力を受付ける。

【００６２】このような入力方法の好適な例としては、ストリーミングサーバ装置１上の情報を特定するためのＵＲＬと、チケットサーバ装置２上の情報に対応した送信規約を特定するためのＵＲＬとを、キーボードから入力させる方法がある。また、これら２つのＵＲＬを含むようなメタファイルを用いてもよい。特に、メタファイルを利用する場合、再生装置３の端末入力手段３１にはメタファイルの蓄積や読込みを行うハードディスク装置等の２次記憶装置と、その２次記憶装置上のファイルを指示するための一般に良く知られたＵＩ（Ｕｓｅｒ Ｉｎｔｅｒｆａｃｅ）手段とを備えればよい。さらに、２次記憶装置の代わりにメモリカード等の補助記憶装置を用いてもよい。

【００６３】その後に、再生装置３はチケット要求処理を行う（図２ステップＳ３２）。具体的には、図３を参照すると、まず、端末入力手段３１においてはステップＡ３１で得られたユーザ入力解釈結果のうち、少なくとも情報識別子とチケットサーバ装置２の位置情報とを含んだチケット受信開始メッセージを生成する（図３ステップＳ１）。

【００６４】このチケット受信開始メッセージがチケット受信手段３６に伝達された後、チケット受信手段３６においては第１のアカウント管理手段３７からクライアント情報を取得する（図３ステップＳ２）。ここで、第１のアカウント管理手段３７は暗号ファイルシステム等を用いて安全に保護された２次記憶装置、またはセキュアメモリカード等の補助記憶装置によって構成されており、第１のアカウント管理手段３７で保持されるクライアント情報はチケットサーバ装置２における課金処理のために必要な情報、例えばユーザＩＤまたはパスワードや、ユーザの公開鍵証明書等を含む。

【００６５】チケット受信手段３６はチケット受信開始メッセージ内の情報識別子と、ストリーミングサーバ装置１の位置情報と、チケットサーバ装置２の位置情報

と、クライアント情報とを含むチケット要求メッセージを生成した後（図３ステップＳ３）、チケットサーバ装置２の位置情報［例えば、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスやホスト名］を基にチケットサーバ装置２との通信を確立し、チケット要求メッセージを送信する（図３ステップＳ４）。

【００６６】チケットサーバ装置２では、まずステップＡ３２で再生装置３から送信されたチケット要求に対する受信処理を行う（図２ステップＡ２１）。より詳細には、図４を参照すると、チケット提供手段２１においては、まずチケット要求メッセージを受信し、そのメッセージをチケット生成手段２２に入力する（図４ステップＳ１１）。

【００６７】チケット生成手段２３においてはチケット要求メッセージ内に記載された情報識別子を抽出して第２の送信規約管理手段２２に入力し、対応する第２の送信規約またはエラーメッセージを取得する（図４ステップＳ１２）。その際、第２の送信規約管理手段２２はその内部に第２の送信規約管理表（図示せず）を備えている。

【００６８】この第２の送信規約管理表は、例えば、図５に示すように、情報識別子をインデックスとして各第２の送信規約の実体の参照／読込みが行えるようになっている。また、情報識別子に合致するようなインデックスがあった時には、対応する第２の送信規約をチケット生成手段２３に出力し、合致するものがなければエラーメッセージを出力するようになっている。ここで、第２の送信規約には、例えば、図６に示すように、情報復号鍵や課金額等が含まれる。

【００６９】チケット生成手段２３は第２の送信規約管理手段２２からの出力を確認し、その出力が第２の送信規約であるか、エラーメッセージであるかを判定する（図４ステップＳ１３）。エラーメッセージであった場合、チケット生成手段２３は不正なチケット要求である旨を伝えるエラーチケットを生成して再生装置３へ送信し、以降の処理を中断する（図４ステップＳ１４）。

【００７０】一方、第２の送信規約であった場合、チケット生成手段２３はチケット要求メッセージに含まれるクライアント情報を抽出し、第２のアカウント管理手段２４に入力してそのクライアント情報の正当性を確認する（図４ステップＳ１５）。

【００７１】ここで、第２のアカウント管理手段２４におけるクライアント情報の正当性の確認方法について、好適な一例としては、クライアント情報として課金処理可能なユーザＩＤとパスワードとの組を用いた場合等において、図７に示すように、予め登録済みの全クライアント情報を記録したアカウント管理表を作成しておく方法がある。この方法の場合には、クライアント情報の入力に応じてアカウント管理表内に合致するものを検索するようにし、合致するものがあれば正当であるとし、または合致するものがなければ不正であると判定する。

【００７２】あるいは、他の好適な例として、クレジットカードやプリペイドカード等の認証に必要な情報（会員番号やカードＩＤ等）をクライアント情報として用いる方法もある。この方法の場合には、上記のようなアカウント管理表は必ずしも必須ではなく、むしろ、図８に示すように、第２のアカウント管理手段２４と決済センタ４とをネットワークで結び、第２のアカウント管理手段２４に入力されたクライアント情報の正当性確認処理を決済センタ４に委譲してもよい。

【００７３】このようにして、クライアント情報の正当性を確認した後、不正なクライアント情報であると判定された場合には、不正なクライアント情報を含む旨を伝えるエラーチケットを生成して再生装置３へ送信し、以降の処理を中断する（図４ステップＳ１６）。一方、正当なクライアント情報であると判定された場合には、次のステップへと処理を移行する。

【００７４】続いて、チケットサーバ装置２は課金処理を行う（図２ステップＡ２２）。より詳細には、図９を参照すると、まず、チケット生成手段２３においては送信規約から課金額を取得する（図９ステップＳ２１）。第２のアカウント管理手段２４は少なくとも課金額とクライアント情報とを課金手段２５に入力し、適切な課金を行う（図９ステップＳ２２）。

【００７５】課金ログ等を残したい時には、この他に、情報識別子等、任意の情報を入力してよい。この際に用いる課金システムは、上述したように、ユーザＩＤとパスワードとの組をクライアント情報として扱う場合、いわゆる会員制課金システムとして動作させればよい。つまり、予めユーザの決済口座を登録しておき、決済口座に一意に対応するユーザＩＤとパスワードとの組を発行しておき、課金手段２５において、当該ユーザＩＤ及びパスワードの組と、課金額とが入力された際に、決済口座宛ての請求書を生成すれば、オフラインで決済することができる。

【００７６】もちろん、金融機関がネットワーク上の決済サーバを持つ場合、例えば、上述したようなクレジットカードやプリペイドカードを用いる場合には、図１０に示すように、課金手段２５と決済サーバ４とをネットワークで結び、クライアント情報と課金額とを決済サーバ４に送信することで、オンライン決済も可能となる。

【００７７】次に、チケットサーバ装置２はチケット生成処理を行う（図２ステップＡ２３）。より詳細には、図１１を参照すると、少なくとも送信規約に記載された情報復号鍵を含む、例えば、図１２に示すようなチケット基底データを生成し（図１１ステップＳ３１）、チケット基底データに対してチケットの正当性証明や再生装置３のユーザ以外の第三者からの参照を防ぐためのセキュリティ的な保護を施したものをチケットとする（図１１ステップＳ３２）。

【００７８】この際、セキュリティ保護の具体的方法として、好適な一例を示すと、まず、チケット生成手段２３内にチケットサーバ装置２の公開鍵証明書を保持しておき、その公開鍵証明書を用いてチケット基底データにディジタル署名を加える。あるいは、再生装置３のユーザにのみ参照可能なようにチケット基底データに暗号化を施す。この際、暗号化に用いる鍵としては、再生装置３の第１のアカウント管理手段３７で保持された特定の鍵をチケット要求メッセージ内に記載しておくか、第２のアカウント管理手段２４におけるクライアント情報の一部として予め登録しておいたものを用いればよい。もちろん、その鍵はチケットサーバ装置２と再生装置３との間で共通のものでもよいし、ＲＳＡ（Ｒｉｖｅｓｔ Ｓｈａｍｉｒ Ａｄｌｅｍａｎ）等の公開鍵暗号系における公開鍵／秘密鍵といった鍵ペアでもよい。

【００７９】その後、上記のようにして生成されたチケットはチケット生成手段２３からチケット提供手段２１へと送られ、チケット提供手段２１から再生装置３へ送信される（図２ステップＡ２４）。

【００８０】再生装置３はチケットサーバ装置２からのチケットに対するチケット受信処理を行う（図２ステップＡ３３）。より詳細には、図１３を参照すると、再生装置３のチケット受信手段３６においてはチケットサーバ装置２から受信したチケットに対してセキュリティ保護を解除する（図１３ステップＳ４１）。例えば、上記のチケット生成処理に記述したように、チケットが再生装置３を使用するユーザのみに参照し得るように暗号化が施されている場合、第１のアカウント管理手段３７に保持された再生装置３に固有の鍵で復号する。あるいは、チケットサーバ装置２の公開鍵証明書を用いてチケットに施されたディジタル署名を確認することによって、チケットの正当性を検証することができる。

【００８１】再生装置３は上記のチケットからチケット基底データを抽出し（図１３ステップＳ４２）、チケット基底データに記載されている情報復号鍵をパケット受信手段３３へ入力し、パケット受信手段３３にてその情報復号鍵を保持する（図１３ステップＳ４３）。

【００８２】この後に、再生装置３は情報要求処理を行う（図２ステップＡ３４）。より詳細には、図１４を参照すると、端末入力手段３１においては少なくとも情報識別子とストリーミングサーバ装置１の位置情報とを含む情報要求開始メッセージが生成され、情報要求手段３２に入力される（図１４ステップＳ５１）。

【００８３】情報要求手段３２は少なくとも情報識別子を含む情報要求メッセージを生成し（図１４ステップＳ５２）、ストリーミングサーバ装置１の位置情報に対応する適切なストリーミングサーバ装置１との通信を確立した後、情報要求メッセージをストリーミングサーバ装置１へ送信する（図１４ステップＳ５３）。この時、その情報要求メッセージを第三者に覗き見されないように、例えばＳＳＬ等の暗号通信方式を用いることもできるが、その方式は必須ではない。

【００８４】ストリーミングサーバ装置１は再生装置３から情報要求メッセージが送られてくると、情報要求確認処理を行う（図２ステップＡ１１）。具体的に、ストリーミングサーバ装置１の情報提供手段１１においては再生装置３から受信した情報要求メッセージを解釈し、情報識別子を抽出した後、パケット生成手段１３へ入力する。この際、上記のように、情報要求メッセージが暗号化されていれば、解釈処理の前に復号処理を行っておく。

【００８５】続いて、ストリーミングサーバ装置１は情報抽出処理を行う（図２ステップＡ１２）。より詳細には、図１５を参照すると、パケット生成手段１３においては情報識別子を第１の送信規約管理手段１２へ入力し、対応する送信規約またはエラーメッセージを取得する（図１５ステップＳ６１）。この時、第１の送信規約管理手段１２は、例えば、その内部に第１の送信規約管理表（図示せず）を備えている。

【００８６】第１の送信規約管理表は、上述した第２の送信規約管理表と同様な構造を持ち、情報識別子をインデックスとして、各第１の送信規約の実体の参照／読込みが行えるようになっている。第１の送信規約管理手段１２は情報識別子に合致するようなインデックスがあれば対応する第１の送信規約をパケット生成手段１３に出力し、合致するものがなければエラーメッセージをパケット生成手段１３に出力するようになっている。また、第１の送信規約はチケットサーバ装置２の第２の送信規約管理手段２２における第２の送信規約と全く同一でなくともよく、少なくとも情報暗号鍵を含んでいれば十分である。

【００８７】その後、パケット生成手段１３は第１の送信規約管理手段１２からの出力が第１の送信規約であるか、エラーメッセージであるかを判定する（図１５ステップＳ６２）。エラーメッセージであった場合、パケット生成手段１３は、例えば、ストリーミングサーバ装置２上で適切な情報がサポートされない旨を伝えるようなエラーメッセージを新たに生成し、情報提供手段１１を介して再生装置３へ送信し、以降の処理を中断する（図１５ステップＳ６６）。

【００８８】一方、第１の送信規約であった場合、パケット生成手段１３は第１の送信規約から情報暗号鍵を抽出し、一時保持しておく（図１５ステップＳ６３）。パケット生成手段１３は情報識別子を情報蓄積手段１４に入力し、対応する情報を取得する（図１５ステップＳ６４）。

【００８９】この時、情報蓄積手段１４は、例えば、その内部に、図１６に示すような情報管理表を保持しており、情報識別子をインデックスとして、動画データや音声データのようなユーザに提供すべき情報の参照／読込

みを行えるようになっている。ユーザに提供すべき情報のフォーマットはＭＰＥＧ２（Ｍｏｖｉｎｇ Ｐｉｃｔｕｒｅ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ ２）やＭＰ３（ＭＰＥＧ ａｕｄｉｏｌａｙｅｒ３）等の任意のものでよく、少なくとも動画フレームや固定長レコード等といった「断片」の系列として、順にアクセス可能であれば十分である。

【００９０】次に、ストリーミングサーバ装置１はパケット送出処理を行う（図２ステップＡ１３）。より詳細には、図１７を参照すると、パケット生成手段１３においては情報蓄積手段１４から上記のような情報の断片を読込みながら、その断片を含んだパケットを生成する（図１７ステップＳ７１）。パケットは上記の断片の他に、パケットの順番を示すシリアル番号等が付加された、例えばＲＦＣ（Ｒｅｑｕｅｓｔ Ｆｏｒ Ｃｏｍｍｅｎｔｓ）２２５０に記載されているようなＲＴＰ（Ｒｅａｌ－ｔｉｍｅ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ）ペイロード等と同様の一般的な構造を持つ。

【００９１】パケット生成手段１３はそうして生成されたパケットに対して、保持しておいた情報暗号鍵を用いて暗号化してセキュアパケットを生成する（図１７ステップＳ７２）。パケット生成手段１３はセキュアパケットを順次、情報提供手段１１を介して再生装置３へ送信する（図１７ステップＳ７３）。

【００９２】パケット生成手段１３はこれら一連の処理（図１７ステップＳ７１～Ｓ７３）を、情報蓄積手段１４から上記のような情報の断片を読込み終えるまで繰り返し行う（図１７ステップＳ７１～Ｓ７４）。パケット生成手段１３は情報蓄積手段１４から上記のような情報の断片を読込み終えた時に情報送信完了メッセージを生成し、情報提供手段１１を介して再生装置３へ送信する（図１７ステップＳ７５）。

【００９３】再生装置３はストリーミングサーバ装置１から情報送信完了メッセージが送られてくると、情報再生処理を行う（図２ステップＡ３５）。より詳細には、図１８を参照すると、まず、再生装置３のパケット受信手段３３においてはストリーミングサーバ装置１の情報提供手段１１からのデータが受信される度に、そのデータがセキュアパケットか否かを判定する（図１８ステップＳ８１）。

【００９４】パケット受信手段３３はセキュアパケットを受信すると、上記のステップＡ３３で保持しておいた情報復号鍵を用いて復号していき（図１８ステップＳ８２）、復号後に得られるパケットを情報再生手段３４へ入力する。情報再生手段３４では入力されたパケットを、パケットに付加されたシリアル番号等を基に情報の一部分を適切に連結し、元の動画データや音声データ等の情報を復元し（図１８ステップＳ８３）、端末出力手段３５を介してユーザにその復元した情報を提示し（図１８ステップＳ８４）、ステップＳ８１に戻る。

【００９５】一方、ストリーミングサーバ装置１の情報提供手段１１から受信されたデータが各種エラーメッセージであるか、情報送信完了メッセージである場合、パケット受信手段３３は情報再生処理を中断し、適切な終了処理を行う（図１８ステップＳ８５）。この終了処理の好適な一例としては、エラーメッセージを受信した場合に、そのエラー内容をユーザに伝えるための警告ダイアログを端末出力手段３５を介して表示する方法や、情報送信完了メッセージを受信した場合に、端末出力手段３５に表示されていた動画表示用のウィンドウを閉じて再生装置３の初期化を行う方法がある。

【００９６】このように、本実施例では、通常、ストリーミング通信を用いた情報販売システムにおけるストリーミングサーバ装置１と再生装置３とに加えて、チケットサーバ装置２を持つように構成しているため、ストリーミングサーバ装置１はユーザ認証処理や課金処理を行う必要がなくなり、販売におけるセキュリティを保ちながら、その応答性能を最大化することができる。

【００９７】また、情報要求処理（図２ステップＡ３４）において、再生装置３からストリーミングサーバ装置１へ伝達される情報要求メッセージには、チケット要求処理（図２ステップＡ３２）におけるチケット要求メッセージと異なり、ユーザを特定したり、課金に必要となるようなクライアント情報が含まれない。こうすることで、チケットサーバ装置２を管理する情報の販売者は、顧客であるユーザのプライバシを厳格に保護することができる。

【００９８】さらに、ストリーミングサーバ装置１が実際に複数台のホスト上で動作している場合でも、チケットサーバ装置２は少なくとも１台のホストで動作していればよいため、情報販売システム全体のスケーラビリティの向上に寄与するとともに、情報の販売者は複数のストリーミングシステムの運用者に情報配信処理を委託することができる。

【００９９】さらにまた、逆に、１台のストリーミングサーバ装置１について、チケットサーバ装置２が実際には複数台のホスト上で動作することも可能であるため、ストリーミングシステムの運用者は複数の情報の販売者から情報配信処理の委託を受けることができる。

【０１００】尚、上記の説明では再生装置３において断片化された情報の受信及び再生を並列的に行うストリーミングデータを販売する場合について述べているが、プログラムや静止画像データ等の販売や貸与等にも適用することができる。その場合、プログラムの販売や貸与等であれば、ストリーミングサーバ装置１の代わりにアプリケーションサーバ等を配置すればよい。

【０１０１】図１９は本発明の一実施例による情報販売システムの具体例を示すブロック図である。図１９において、本発明の一実施例による情報販売システムではチケットサーバ装置２を運用する情報の販売者Ｐ２と、ス

トリーミングサーバ装置１を運用するストリーミングシステム運用者Ｐ１との間で、情報配信処理の委託契約を結び、再生装置３を用いる任意のユーザＰ３と情報の販売者Ｐ１との間で、情報の購入契約を結ぶ。

【０１０２】その後、ユーザＰ３が再生装置３及びストリーミングサーバ装置１を介して、ストリーミングシステム運用者Ｐ１から情報の提供を受ける時、チケットサーバ装置２からチケットを取得し、それと引き換えに情報の販売者Ｐ２に対してその情報の代金が支払われ、情報の販売者Ｐ２はストリーミングシステム運用者Ｐ１に対して、委託契約に基づく配信手数料を支払う。

【０１０３】図２０は図１９の情報販売システムにおける情報販売手続きを示すフローチャートであり、図２１は図１９のチケットサーバ装置２において課金履歴に基いて課金処理を行うための構成の一例を示すブロック図である。これら図１９及び図２０を参照して図１９の情報販売システムにおける情報配信処理の委託契約及び配信手数料の授受を含む情報の販売方法について説明する。

【０１０４】まず、情報の販売者Ｐ２は任意のストリーミングシステム運用者Ｐ１と、情報の配信手数料の取り決めを行う（図２０ステップＢ１）。この取り決めの内容は個々の情報について異なってもよいし、配信処理１回あたりの料金を定めてもよいし、特定の有効期間を定めるものでもよいし、あるいはこれらの組み合わせでもよい。

【０１０５】例えば、「配信処理１回あたり５０円を、情報の販売者から、ストリーミングシステムの運用者に支払う。但し、動画Ａについては、特別に３０円／回とする」という内容でもよいし、「２００１年8月１日より３ヶ月間、配信を行うものとし、情報の販売者Ｐ２から、ストリーミングシステム運用者Ｐ１に対して、配信手数料として、１００万円支払う。」というような内容でもよい。

【０１０６】上記のような委託契約を交わした後、情報の販売者Ｐ２は、販売の対象となる情報とそれに対応する送信規約とをストリーミングシステム運用者Ｐ１に渡す（図２０ステップＢ２）。同時に、その送信規約にユーザＰ３から徴収すべき代金（課金額）等の情報を加えたものをチケットサーバ装置２の第２の送信規約管理手段２２に登録しておく（図２０ステップＢ３）。

【０１０７】ストリーミングシステム運用者Ｐ１は情報の販売者Ｐ２から受取った情報を、ストリーミングサーバ装置１の情報蓄積部１４に登録し、さらに送信規約を第１の送信規約管理手段１２に登録する（図２０ステップＢ４）。

【０１０８】このようにして、委託契約とそれに伴うシステム設定とを行った後、情報の販売者Ｐ２は情報に対応する情報識別子と、ストリーミングサーバ装置１の位置情報と、チケットサーバ装置２の位置情報とを含んだ、例えばメタファイルを作成する（図２０ステップＢ５）。情報の販売者Ｐ２はそのメタファイルを要求するユーザＰ３があれば、このユーザＰ３との間で、販売（購入）契約を結ぶ（図２０ステップＢ６）。

【０１０９】販売契約を結ぶにあたっては情報の代金が情報の販売者Ｐ２からユーザＰ３に提示され，その決済に必要な情報をユーザＰ３が情報の販売者Ｐ２に返す。この時、決済に必要な情報として、クレジットカードの会員番号や、銀行口座の番号等を逐一入力する形態でもよいし、情報の販売者Ｐ２によって予め用意されたＷｅｂシステム等において、そうした決済用情報をユーザＩＤやパスワード等とともに登録しておき、各購入契約にあたってはユーザＩＤやパスワードを入力するという形態でもよい。いずれの形態においても、決済用情報と、もしあればそれに関連付けられたユーザＩＤ等の情報をチケットサーバ装置２のアカウント管理手段２４に登録しておく。

【０１１０】ユーザＰ３と情報の販売者Ｐ２との間で販売契約が成立した後、メタファイルがユーザＰ３に配布される（図２０ステップＢ７）。その後、このメタファイルが再生装置３に入力されると、再生装置３はメタファイルに記述されたストリーミングサーバ装置１及びチケットサーバ装置２との間で、上述したステップＡ３１～Ａ３５までの動作を行い、情報の提供を受ける（図２０ステップＢ８）。

【０１１１】この時、特にチケット要求処理（図２ステップＡ３２）において、チケット要求メッセージには決済用情報に関連付けから得たユーザＩＤもしくは決済用情報そのものであるクレジットカード会員番号等がクライアント情報の一部として含まれ、課金処理（図２ステップＡ２２）において、当該ユーザＩＤ等に関連付けられた決済用情報あるいはチケット要求メッセージに含まれる決済用情報そのものに基づいて課金処理が行われる。ユーザＩＤ等を用いる場合には上記のステップＢ６において、アカウント管理手段２４で関連付けられた決済用情報が登録されているので、これを用いればよい。

【０１１２】その後、情報の販売者Ｐ２はストリーミングシステムの運用者Ｐ１に、上記のステップＢ１で交わした契約に基づいて、所定の配信手数料を支払う（図２０ステップＢ９）。特に、情報の配信処理１回毎に手数料が発生するような契約形態である場合には、チケットサーバ装置２の課金手段２５における課金処理（図２ステップＡ２２）のログデータを基に、一定期間内の配信手数料を算出することができる。

【０１１３】このため、図２１に示すように、課金手段２５と情報の販売者Ｐ２が別途用意した課金ログデータベース５とを接続しておき、課金処理（図２ステップＡ２２）の処理時に、少なくとも情報識別子と課金額とが課金ログデータベース５に蓄積されるようにしておけばよい。

【０１１４】上記のステップＢ１で交わした契約に、期間等の契約失効の条件がある場合、失効時に上記のステップＢ３でチケットサーバ装置２の送信規約管理部２３に登録した第２の送信規約を削除することで、情報の販売者Ｐ１による契約解除を行うことができる。

【０１１５】図２２は本発明の他の実施例による情報販売システムの構成を示すブロック図である。図２２において、本発明の他の実施例による情報販売システムはチケットサーバ装置２に代えて第２のチケットサーバ装置６を備えた以外は図１に示す本発明の一実施例による情報販売システムと同様の構成となっており、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の一実施例と同様である。つまり、図示していないが、ストリーミングサーバ装置１及び再生装置３の構成は図１に示すストリーミングサーバ装置１及び再生装置３の構成と同じである。

【０１１６】第２のチケットサーバ装置６は、図１に示すチケットサーバ装置２と比して、第２の送信規約管理手段２２に代えて、送信規約グループ管理手段６１と、Ｎ個の第２の送信規約管理手段２２－１～２２－Ｎとを備える点で異なる。尚、記録媒体２６には送信規約グループ管理手段６１と、Ｎ個の第２の送信規約管理手段２２－１～２２－Ｎとにおいてそれぞれ実行されるプログラムも格納されているものとする。

【０１１７】送信規約グループ管理手段６１はチケット生成手段２３から少なくとも第２の情報識別子の入力を受け、適切な第２の送信規約管理手段（例えば、第ｋ番目の第２の送信規約管理手段２２－ｋ）を選択し、選択した第２の送信規約管理手段２２－ｋへ情報識別子を入力し、その応答として得られた第２の送信規約もしくはエラーメッセージをチケット生成手段２３へ出力する。

【０１１８】また、それぞれの第２の送信規約管理手段２２－１～２２－Ｎは送信規約グループ管理手段６１から情報識別子の入力を受けて、図１に示す第２の送信規約管理手段２２と同様にして、その情報識別子に対応する第２の送信規約を検索し、検索した第２の送信規約を送信規約グループ管理手段６１へ出力する。

【０１１９】図２３は本発明の他の実施例による情報販売システムの動作を示すフローチャートであり、図２４は図２３の第２のチケット要求確認処理を示すフローチャートであり、図２５は本発明の他の実施例における第２の情報識別子のフォーマットの一例を示す図であり、図２６は本発明の他の実施例における送信規約グループ管理表の一例を示す図である。

【０１２０】これら図２２～図２６を参照して本発明の他の実施例による情報販売システムの動作について説明する。尚、図２３及び図２４に示す処理はストリーミングサーバ装置１、第２のチケットサーバ装置６、再生装置３各々の各手段が記録媒体１５，２６，３８に夫々格納されたプログラムを実行することで実現される。

【０１２１】ここで、図２３に示す第２のチケットサーバ装置６の動作は、図２に示すチケットサーバ装置２の動作におけるチケット確認処理（図２ステップＡ２１）の代わりに、第２のチケット確認処理（図２３ステップＡ７１）を行うようにした点で本発明の一実施例による情報販売システムと異なる。

【０１２２】ステップＡ７１をより詳細に述べると、図２４に示すように、まず、図２のチケット確認処理（図２ステップＡ２１）と同様に、第２のチケットサーバ装置６においてはチケット提供手段２１で受信したチケット要求がチケット生成手段２３に伝達される（図２４ステップＳ９１）。

【０１２３】その後、チケット生成手段２３はチケット要求に記載された第２の情報識別子を抽出して送信規約グループ管理手段６１へ入力する（図２４ステップＳ９２）。送信規約グループ管理手段６１は第２の情報識別子を運用者識別子と情報識別子（第１の情報識別子）（本発明の一実施例におけるものと同一）とに分割する（図２４ステップＳ９３）。

【０１２４】送信規約グループ管理手段６１は運用者識別子から適切なｋ番目の第２の送信規約管理手段２２－ｋを選択し、第１の情報識別子を第２の送信規約管理手段２２－ｋに入力し、第２の送信規約もしくはエラーメッセージを取得し、チケット生成手段２３へ出力する（図２４ステップＳ９４）。

【０１２５】この後、チケット生成手段２３は、上述した本発明の一実施例と同様に、第２の送信規約かエラーメッセージかの判定（図２４ステップＳ９５）と、エラー処理（図２４ステップＳ９６）もしくはチケット要求の正当性確認（図２４ステップＳ９６）を行う。

【０１２６】尚、第２の情報識別子は、図２５に示すように、予めストリーミングシステム運用者毎に定められた運用者識別子（例えば、ストリーミングシステム運用者のドメイン名等）と、第１の情報識別子を連結したフォーマットを持っており、再生装置３及びストリーミングサーバ装置１においては第１の情報識別子と全く同様に扱われる。また、送信規約グループ管理手段６１はその内部に、図２６に示すように、運用者識別子とそれに対応する第２の送信規約管理手段２２－ｋとの関連付け（例えば、ポインタ）を保持する表を保持している。

【０１２７】このように、情報の販売者が複数のストリーミングシステム運用者に対して、委託契約を結ぶ際に、ストリーミングシステム運用者毎に異なる契約内容を持たせたり、あるいは異なる情報の委託及び管理を行うことができる。

【０１２８】図２７は本発明の別の実施例による情報販売システムの構成を示すブロック図である。図２７において、本発明の別の実施例による情報販売システムはストリーミングサーバ装置１に代えて第２のストリーミングサーバ装置７を備え、再生装置３に代えて第２の再生

装置８を備えるようにした以外は図１に示す本発明の一実施例による情報販売システムと同様であり、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の一実施例と同様である。つまり、図示していないが、チケットサーバ装置２の構成は図１に示すチケットサーバ装置２の構成と同じである。

【０１２９】第２のストリーミングサーバ装置７は第１のセッション鍵確立手段７１を設け、パケット生成手段１３に代えて第２のパケット生成手段７２を設けた以外は図１に示すストリーミングサーバ装置１と同様の構成である。尚、記録媒体１５には第１のセッション鍵確立手段７１と、第２のパケット生成手段７２とにおいてそれぞれ実行されるプログラムも格納されているものとする。

【０１３０】第１のセッション鍵確立手段７１は第２の再生装置８からのセッション鍵要求メッセージを受信すると、適当なセッション鍵を発生して保持し、そのセッション鍵を第２の再生装置８に送信する。また、第１のセッション鍵確立手段７１は第２のパケット生成手段７２からの要求に応じて、そのセッション鍵を第２のパケット生成手段７２に出力する。ここで、セッション鍵とは情報暗号鍵を変形するための情報を示しており、例えば、乱数やワンタイムパスワード等がある。すなわち、セッション鍵は第２の再生装置８との間のセッション毎に使用される使い捨ての鍵情報である。

【０１３１】第２のパケット生成手段７２は情報提供手段１１から情報識別子の入力を受けると、その情報識別子を基に情報暗号鍵を取得するか、あるいはエラーメッセージを取得する。また、第２のパケット生成手段７２は情報識別子を情報蓄積手段１４に入力し、ユーザに提供すべき情報を取得する。

【０１３２】さらに、第２のパケット生成手段７２は第１のセッション鍵確立手段７１からセッション鍵を取得し、そのセッション鍵を情報暗号鍵と統合する。さらにまた、第２のパケット生成手段７２は情報と、統合された情報暗号鍵とから生成したセキュアパケットを順に情報提供手段１１に出力するか、あるいはエラーメッセージを情報提供手段１１に出力する。

【０１３３】第２の再生装置８は第２のセッション鍵確立手段８１を設け、パケット受信手段３５に代えて第２のパケット受信手段８２を設けた以外は図１に示す再生装置３と同様の構成となっている。尚、記録媒体３８には第２のセッション鍵確立手段８１と、第２のパケット受信手段８２とにおいてそれぞれ実行されるプログラムも格納されているものとする。

【０１３４】第２のセッション鍵確立手段８１は第２のストリーミングサーバ装置７の第１のセッション鍵確立手段７１に対してセッション鍵要求メッセージを送信し、第１のセッション鍵確立手段７１からセッション鍵を受信して保持する。また、第２のセッション鍵確立手段８１は第２のパケット受信手段８２からの要求に応じて、受信したセッション鍵を第２のパケット受信手段８２に出力する。

【０１３５】第２のパケット受信手段８２は第２のストリーミングサーバ装置７からセキュアパケットを受信した際、チケット受信手段３６から入力された情報復号鍵と、第２のセッション鍵確立手段８１から取得されるセッション鍵とを用いて、そのセキュアパケットを復元した結果（復元パケット）を情報再生手段３４に出力する。

【０１３６】図２８は本発明の別の実施例による情報販売システムの動作を示すフローチャートであり、図２９は図２８の第２の情報抽出処理を示すフローチャートであり、図３０は図２８のセッション鍵要求処理を示すフローチャートであり、図３１は図２８のセッション鍵生成処理を示すフローチャートである。

【０１３７】図３２は図２８のセッション鍵受信処理を示すフローチャートであり、図３３は図２８の第２のパケット送出処理を示すフローチャートであり、図３４は図２８の第２の情報再生処理を示すフローチャートである。

【０１３８】これら図２７～図３４を参照して本発明の別の実施例による情報販売システムの動作について説明する。尚、図２８～図３４に示す処理は第２のストリーミングサーバ装置７、チケットサーバ装置２、第２の再生装置８各々の各手段が記録媒体１５，２６，３８に夫々格納されたプログラムを実行することで実現される。

【０１３９】ここで、図２８において、ユーザ入力開始処理（図２ステップＡ３１）から情報要求確認処理（図２ステップＡ１１）までの処理は本発明の一実施例による情報販売システムと同一の処理を行う。その後、本発明の一実施例による情報販売システムの動作における情報抽出処理（図２ステップＡ１２）の代わりに、第２の情報抽出処理（図２８ステップＡ７１）が行われ、その後、第２の再生装置８と第２のストリーミングサーバ装置７との間で、セッション鍵要求処理（図２８ステップＡ８１）と、セッション鍵生成処理（図２８ステップＡ７２）と、セッション鍵受信処理（図２８ステップＡ８２）とが行われる点で本発明の一実施例と異なる。

【０１４０】また、本発明の一実施例による情報販売システムの動作におけるパケット送出処理（図２ステップＡ１３）及び情報再生処理（図２ステップＡ３５）の代わりに、第２のパケット送出処理（図２８ステップＡ７３）と第２の情報再生処理（図２８ステップＡ８３）とが行われる点で本発明の一実施例と異なる。尚、以下の説明ではセッション鍵として乱数を用いるものとする。

【０１４１】まず、第２のストリーミングサーバ装置７における第２の情報抽出処理（図２８ステップＡ７１）を、図２９を参照しながら、より詳細に説明すると、まず、本発明の一実施例による情報販売システムの動作と

同様の情報抽出処理（図２９ステップＳ１０１～Ｓ１０４，Ｓ１０６）が行われた後、情報抽出完了メッセージを生成し、第２の再生装置８の情報要求手段３２に送信する（図２９ステップＳ１０５）。

【０１４２】その後、第２の再生装置８ではセッション鍵要求処理（図２８ステップＡ８１）が行われる。図３０を参照しながら、より詳細に説明すると、情報要求手段３２においては情報抽出完了メッセージを受信した際、セッション鍵確立開始メッセージを生成し、そのセッション鍵確立開始メッセージを第２のセッション鍵確立手段８１に入力する（図３０ステップＳ１１１）。

【０１４３】第２のセッション鍵確立手段８１はセッション鍵要求メッセージを生成し、第２のストリーミングサーバ装置７の第１のセッション鍵確立手段７１へそのセッション鍵要求メッセージを送信する（図３０ステップＳ１１２）。その際、情報要求処理（図２８ステップＡ３４）で確立された通信路とは、別の通信路を用いてもよい。

【０１４４】第２のストリーミングサーバ装置７ではセッション鍵生成処理（図２８ステップＡ７２）が行われる。図３１を参照しながら、より詳細に説明すると、第１のセッション鍵確立手段７１はセッション鍵要求メッセージを受信し（図３１ステップＳ１２１）、その後、乱数を生成し、それを内部的に一時保持する（図３１ス＊＊テップＳ１２２）。第１のセッション鍵確立手段７１は乱数を第２の再生装置８の第２のセッション鍵確立手段８１へ送信する（図３１ステップＳ１２３）。

【０１４５】その後、第２の再生装置８ではセッション鍵受信処理（図２８ステップＡ８２）が行われる。図３２を参照しながら、より詳細に説明すると、第２のセッション鍵確立手段８１は乱数を受信し（図３２ステップＳ１３１）、その乱数を内部的に一時保持する（図３２ステップＳ１３２）。その後、第２のセッション鍵確立手段８１はセッション鍵受信完了メッセージを第１のセッション鍵確立手段７１に送信する（図３２ステップＳ１３３）。

【０１４６】第２のストリーミングサーバ装置７では第２のパケット送出処理（図２８ステップＡ７３）が行われる。図３３を参照しながら、より詳細に説明すると、第２のパケット生成手段７２においては、図１に示すパケット生成手段１３と同様に、情報の断片の読込みとパケット生成とを行う（図３３ステップＳ１４１）。

【０１４７】第２のパケット生成手段７２は第１のセッション鍵確立手段７１から乱数Ｒを取得し（図３３ステップＳ１４２）、保持している情報暗号鍵Ｋとともに、適当な統合化関数Ｆにかけ、その値Ｆ（Ｋ，Ｒ）に情報暗号鍵Ｋを置換える（図３３ステップＳ１４３）。

【０１４８】統合化関数Ｆの好適な例としては、

Ｆ（Ｋ，Ｒ）＝Ｋ　ＸＯＲ　Ｒ　……（１）

Ｆ（Ｋ，Ｒ）＝Ｅ［Ｒ］（Ｋ）　……（２）

Ｆ（Ｋ，Ｒ）＝Ｈ（Ｋ，Ｒ）　……（３）

等を用いることができる。尚、（１）式においてＸＯＲは排他的論理和を示し、（２）式においてＥは乱数Ｒを鍵とする暗号化関数を示し、（３）式においてＨは情報暗号鍵Ｋ及び乱数Ｒの連結を入力とする一方向性ハッシュ関数を示している。

【０１４９】第２のパケット生成手段７２は値Ｆ（Ｋ，Ｒ）を鍵として、ステップＳ１４１で生成したパケットを暗号化し、セキュアパケットを生成する（図３３ステップＳ１４４）。このようにして生成されたセキュアパケットを、順次、情報提供手段１１を介して第２の再生装置８へ送信する（図３３ステップＳ１４５）。

【０１５０】第２のパケット生成手段７２はこれら一連の処理を情報の断片の読込みが完了するまで繰り返し行い（図３３ステップＳ１４１～Ｓ１４６）、未送出の断片が無くなった時、情報送信完了メッセージを生成し、情報提供手段１１を介して第２の再生装置８へ送信する（図３３ステップＳ１４７）。

【０１５１】その後、第２の再生装置８で第２の情報再生処理（図２８ステップＡ８３）が行われる。図３４を参照しながら、より詳細に説明すると、まず、第２のパケット受信手段８２では受信データがセキュアパケットか否かの判別を行い（図３４ステップＳ１５１）、もし必要ならば図１に示す再生装置３と同様に、例外処理を行って終了する（図３４ステップＳ１５８）。

【０１５２】受信データがセキュアパケットであった場合、第２のパケット受信手段８２は第２のセッション鍵確立手段８１で保持されている乱数を取得する（図３４ステップＳ１５２）。本発明の一実施例による動作と同様のチケット受信処理（図２ステップＡ３３）によって、予め第２のパケット受信手段８２で保持されている情報復号鍵Ｋと乱数Ｒとをともに、統合化関数Ｆに掛け、その値Ｆ（Ｋ，Ｒ）に情報復号鍵Ｋを置換える（図３４ステップＳ１５３）。

【０１５３】その後、第２のパケット受信手段８２は値Ｆ（Ｋ，Ｒ）を用いてセキュアパケットを受信された順に復号していく（図３４ステップＳ１５４）。第２のパケット受信手段８２は、本発明の一実施例と同様にして、復元パケットから元の動画データや音声データ等の情報に復元し（図３４ステップＳ１５５）、端末出力手段３５を介してユーザにその情報を提示しながら（図３４ステップＳ１５６）、ステップＳ１５１以降の処理を繰り返し行う（図３４ステップＳ１５１～Ｓ１５７）。

【０１５４】このように、第２のストリーミングサーバ装置７と第２の再生装置８との間で同じ情報を提供する複数の通信（＝セッション）について、セッション毎にセキュアパケットの暗号鍵及び復号鍵が異なるため、そ

のセッションを傍受する第三者に対して、より高いセキュリティを実現することができる。

【０１５５】尚、上記のステップＡ８１、Ａ７２、Ａ８２に記載したセッション鍵の確立に係る処理について、特に通信処理がセキュアパケットの送受信に係る通信路と異なる通信路を用いて行われる場合、セキュアパケットを複数台の第２の再生装置８に対してマルチキャスト配信することもできる。この場合、セッション鍵生成処理（図２８ステップＡ７２）において、第２のストリーミングサーバ装置７の第１のセッション鍵確立手段７１において、第２の再生装置８毎に異なる乱数を発生させるのではなく、情報をマルチキャスト配信する度に異なる乱数を発生させればよい。＊

＊【０１５６】また、上記のステップＡ８１、Ａ７２、Ａ８２に記載したセッション鍵の確立に係る処理について、第２の再生装置８の第２のセッション鍵確立手段８１で、乱数Ｒ２を発生させ、セッション鍵要求メッセージに乱数Ｒ２を含めることもできる。さらに、ステップＡ７２と同様に、第２のストリーミングサーバ装置７の第１のセッション鍵確立手段７１でも乱数Ｒ１を発生させ、第２の再生装置８に送信してもよい。この場合、ステップＡ７３，Ａ８３において、情報暗号鍵Ｋ１及び情報復号鍵Ｋ２を置き換えるための鍵を生成する式を、それぞれに用いればよい。

【０１５７】この場合の第２の統合化関数Ｆ’及びＦ”は

$$F'(K1, R1, R2) = F(K1, DH1(R1, R2)) \quad \cdots\cdots (4)$$

$$F''(K2, R1, R2) = F(K2, DH2(R1, R2)) \quad \cdots\cdots (5)$$

をそれぞれに用いればよい。

【０１５８】尚、関数ＤＨ１，ＤＨ２は、

$$R1 = g\hat{\ } r1 \bmod N \quad \cdots\cdots (6)$$

$$R2 = g\hat{\ } r2 \bmod N \quad \cdots\cdots (7)$$

$$DH1(R1, R2) = (R2)\hat{\ } r1 \bmod N \quad \cdots\cdots (8)$$

$$DH2(R1, R2) = (R1)\hat{\ } r2 \bmod N \quad \cdots\cdots (9)$$

という（６）式～（９）式で示されるような関数であり、これは、Ｄｉｆｆｉｅ及びＨｅｌｌｍａｎらによって「ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎＩｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ」（ｖ．ＩＴ－２２，ｎ．６，１９７６）に記載された鍵交換法（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換法）として、一般によく知られるものである。

【０１５９】ここで、（６）式においてＮはある大きな整数、ｇは整数群Ｚ（Ｎ）上の原始元であるようなある定数、ｒ１はある乱数、＾はべき乗、ｍｏｄは剰余を示している。また、（７）式においてｒ２はある乱数を示している。こうすることで、さらに高いセキュリティを実現することができる。

【０１６０】このように、情報の販売者が自己の所有する情報の販売条件を送信規約として管理するためのチケットサーバ装置を備えることによって、情報の販売者がストリーミングシステムの運用者に情報の配信業務を委託する際に、情報の販売者が自己の所有する情報の販売条件を自由に設定することができる。

【０１６１】また、利用者認証処理や課金処理をストリーミングサーバ装置１，７とは独立したチケットサーバ装置２，６で行うことによって、情報の提供時に、ストリーミングシステムのパフォーマンスを低下させずに、利用者認証処理や課金処理を安全に行うことができる。

【０１６２】

【０１６３】

【発明の効果】以上説明したように本発明の情報販売方法は、情報を暗号化してユーザに提供するための情報暗号鍵を含んだ第１の送信規約を管理するための第１の送信規約管理手段をストリーミングサーバ装置に設け、暗号化された情報を復号して再生可能とするための情報復号鍵を含んだ送信規約を管理するための第２の送信規約管理手段をチケットサーバ装置に設けることによって、情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、情報の販売者が自己の所有する情報の販売条件（価格や利用者制限）を自由に設定することができるという効果が得られる。

【０１６４】また、本発明の他の情報販売方法は、情報をユーザに販売するにあたって当該ユーザの認証処理を行うための第２のアカウント管理手段と、ユーザに対する課金処理を行う課金手段とをチケットサーバ装置に設け、要求された情報をユーザに送信するにあたって単に暗号化された情報の送出を行う情報提供手段をストリーミングサーバ装置に設けることによって、ストリーミングシステムが行う情報の送信処理のパフォーマンスを低下させることなく、利用者認証処理や課金処理を行うことができるという効果が得られる。

【０１６５】さらに、本発明の別の情報販売方法は、情報の販売者が情報の代金をユーザから徴収した時に当該情報の復号鍵をユーザに与え、送信規約の一方を管理するストリーミングシステム運用者に対して所定の委託契約に基づいた配信手数料を支払うことによって、情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、利用者から得られる利益を、情報の販売者とストリーミングシステムの運用者との間で公正に分配することができるという効果が得られ

る。

【図面の簡単な説明】

【図１】本発明の一実施例による情報販売システムの構成を示すブロック図である。

【図２】本発明の一実施例による情報販売システムの動作を示すフローチャートである。

【図３】図２のチケット要求処理を示すフローチャートである。

【図４】図２のチケット要求確認処理を示すフローチャートである。

【図５】本発明の一実施例における送信規約管理表の一例を示す図である。

【図６】本発明の一実施例における送信規約の一例を示す図である。

【図７】本発明の一実施例におけるアカウント管理表の一例を示す図である。

【図８】図１のチケットサーバ装置における決済センタヘアカウンティング情報の正当性確認を委譲するための構成の一例を示す図である。

【図９】図２の課金処理を示すフローチャートである。

【図１０】図１のチケットサーバ装置における決済センタを用いて課金処理を行うための構成の一例を示す図である。

【図１１】図２のチケット生成処理を示すフローチャートである。

【図１２】本発明の一実施例におけるチケットのフォーマットの一例を示す図である。

【図１３】図２のチケット受信処理を示すフローチャートである。

【図１４】図２の情報要求処理を示すフローチャートである。

【図１５】図２の情報抽出処理を示すフローチャートである。

【図１６】本発明の一実施例における情報管理表の一例を示す図である。

【図１７】図２のパケット送出処理を示すフローチャートである。

【図１８】図２の情報再生処理を示すフローチャートである。

【図１９】本発明の一実施例による情報販売システムの具体例を示すブロック図である。

【図２０】図１９の情報販売システムにおける情報販売手続きを示すフローチャートである。

【図２１】図１９のチケットサーバ装置において課金履歴に基いて課金処理を行うための構成の一例を示すブロック図である。

【図２２】本発明の他の実施例による情報販売システムの構成を示すブロック図である。

【図２３】本発明の他の実施例による情報販売システムの動作を示すフローチャートである。

【図２４】図２３の第２のチケット要求確認処理を示すフローチャートである。

【図２５】本発明の他の実施例における第２の情報識別子のフォーマットの一例を示す図である。

【図２６】本発明の他の実施例における送信規約グループ管理表の一例を示す図である。

【図２７】本発明の別の実施例による情報販売システムの構成を示すブロック図である。

【図２８】本発明の別の実施例による情報販売システムの動作を示すフローチャートである。

【図２９】図２８の第２の情報抽出処理を示すフローチャートである。

【図３０】図２８のセッション鍵要求処理を示すフローチャートである。

【図３１】図２８のセッション鍵生成処理を示すフローチャートである。

【図３２】図２８のセッション鍵受信処理を示すフローチャートである。

【図３３】図２８の第２のパケット送出処理を示すフローチャートである。

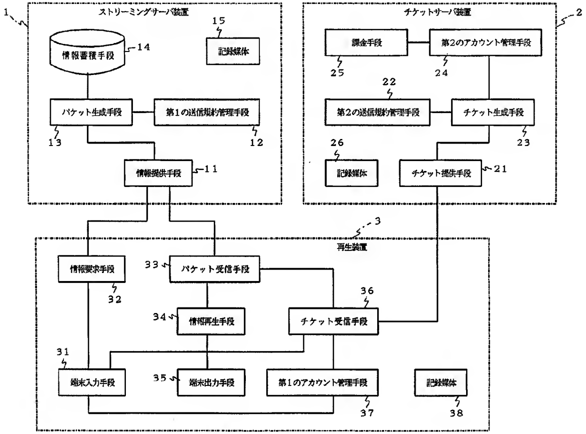
【図３４】図２８の第２の情報再生処理を示すフローチャートである。

【符号の説明】

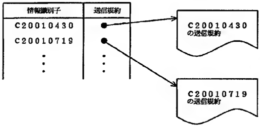
１　ストリーミングサーバ装置
２　チケットサーバ装置
３　再生装置
４　決済センタ
５　課金ログデータベース
６　第２のチケットサーバ装置
７　第２のストリーミングサーバ装置
８　第２の再生装置
１１　情報提供手段
１２　第１の送信規約管理手段
１３　パケット生成手段
１４　情報蓄積手段
２１　チケット提供手段
２２，２２－１～２２－Ｎ　第２の送信規約管理手段
２３　チケット生成手段
２４　第２のアカウント管理手段
２５　課金手段
３１　端末入力手段
３２　情報要求手段
３３　パケット受信手段
３４　情報再生手段
３５　端末出力手段
３６　チケット受信手段
３７　第１のアカウント管理手段
６１　第２の送信規約管理手段
７１　第１のセッション鍵確立手段
７２　第２のパケット生成手段

８１　第２のセッション鍵確立手段
８２　第２のパケット受信手段
Ｐ１　ストリーミングシステム運用者
Ｐ２　情報の販売者
Ｐ３　ユーザ

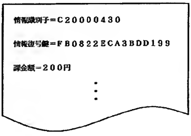
【図１】



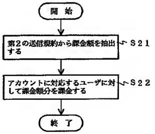
【図５】



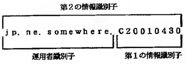
【図６】



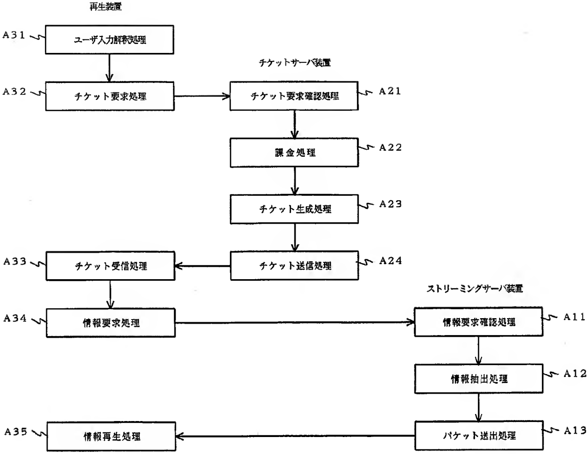
【図９】



【図２５】



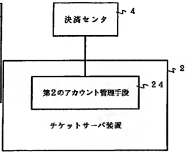
【図2】



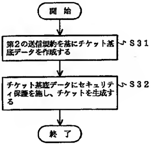
【図7】

情報識別子	パスワード	口座番号	・・・
⋮	⋮	⋮	⋮
U1002011	WB30B&X	09382653	・・・
U1002012	GM^2jfnb	13923567	・・・
⋮	⋮	⋮	⋮

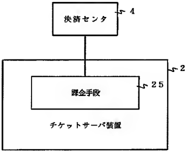
【図8】



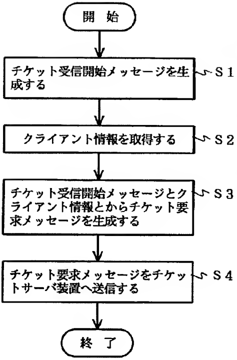
【図11】



【図10】



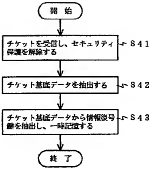
【図３】



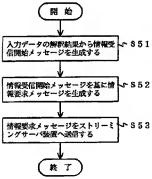
【図１２】

シリアル番号	TK2001080112345
情報識別子	C20010430
ユーザID	U1002011
情報復号鍵	FB0822ECA3BDD199
発行年月日	2001年08月01日
有効期限	2001年08月01日

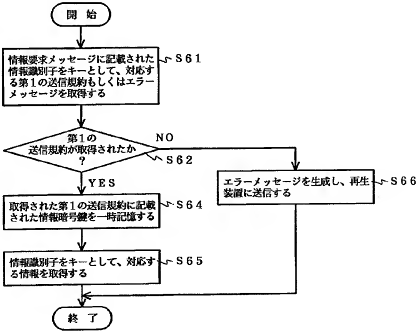
【図１３】



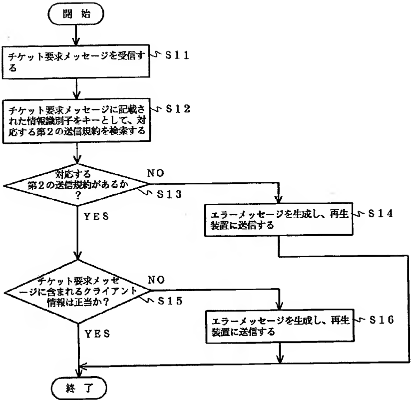
【図１４】



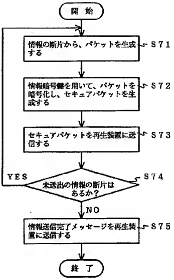
【図１５】



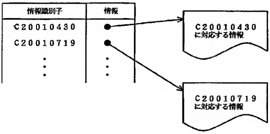
【図４】



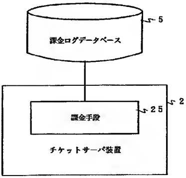
【図１７】



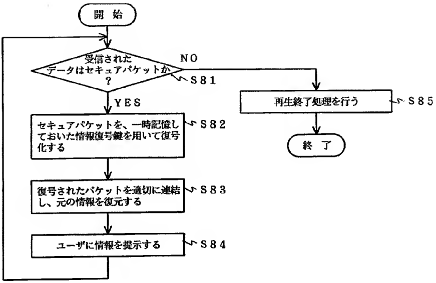
【図１６】



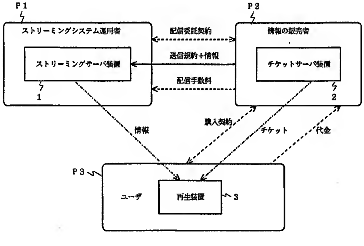
【図２１】



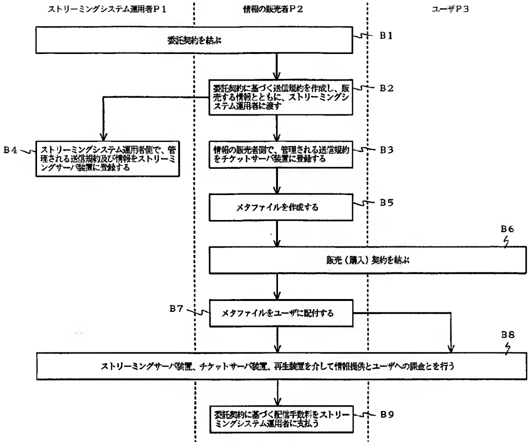
【図１８】


開始
受信されたデータはセキュアパケットか？
NO
S81
YES
再生終了処理を行う
S85
終了
セキュアパケットを、一時記憶しておいた情報復号鍵を用いて復号化する
S82
復号されたパケットを適切に連結し、元の情報を復元する
S83
ユーザに情報を提示する
S84

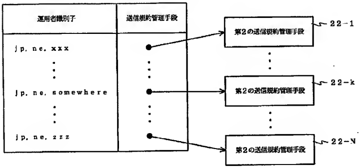
【図１９】


P1
ストリーミングシステム運用者
ストリーミングサーバ装置
1
P2
情報の販売者
チケットサーバ装置
2
配信委託契約
送信規約＋情報
配信手数料
情報
購入契約
チケット
代金
P3
ユーザ
再生装置
3

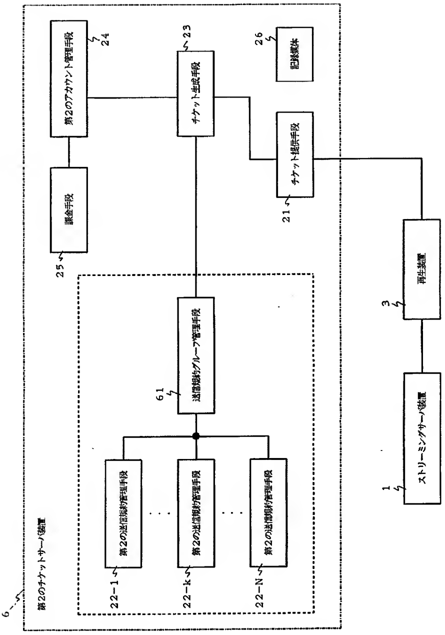
【図２０】


ストリーミングシステム運用者Ｐ１
情報の販売者Ｐ２
ユーザＰ３
委託契約を結ぶ
Ｂ１
委託契約に基づく送信規約を作成し、販売する情報とともに、ストリーミングシステム運用者に渡す
Ｂ２
Ｂ４
ストリーミングシステム運用者側で、管理される送信規約及び情報をストリーミングサーバ装置に登録する
情報の販売者側で、管理される送信規約をチケットサーバ装置に登録する
Ｂ３
メタファイルを作成する
Ｂ５
Ｂ６
販売（購入）契約を結ぶ
Ｂ７
メタファイルをユーザに配付する
Ｂ８
ストリーミングサーバ装置、チケットサーバ装置、再生装置を介して情報提供とユーザへの課金とを行う
委託契約に基づく配信手数料をストリーミングシステム運用者に支払う
Ｂ９

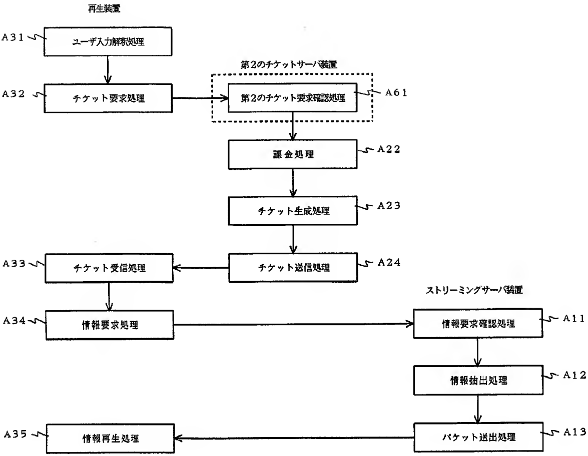
【図２６】


運用者識別子
送信規約管理手段
jp. ne. xxx
jp. ne. somewhere
jp. ne. zzz
第２の送信規約管理手段
22－1
22－k
22－N

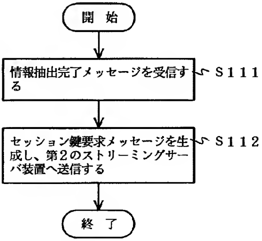
【図２２】


第2のチケットサーバ装置
6
第2のアカウント管理手段
24
チケット生成手段
23
記録媒体
26
チケット提供手段
21
課金手段
25
送信規約グループ管理手段
61
第2の送信規約管理手段
22−1
第2の送信規約管理手段
22−k
第2の送信規約管理手段
22−N
再生装置
3
ストリーミングサーバ装置
1

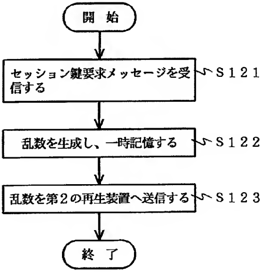
【図２３】


再生装置
A31
ユーザ入力解釈処理
A32
チケット要求処理
第2のチケットサーバ装置
第2のチケット要求確認処理
A61
課金処理
A22
チケット生成処理
A23
チケット送信処理
A24
A33
チケット受信処理
ストリーミングサーバ装置
A34
情報要求処理
情報要求確認処理
A11
情報抽出処理
A12
A35
情報再生処理
パケット送出処理
A13

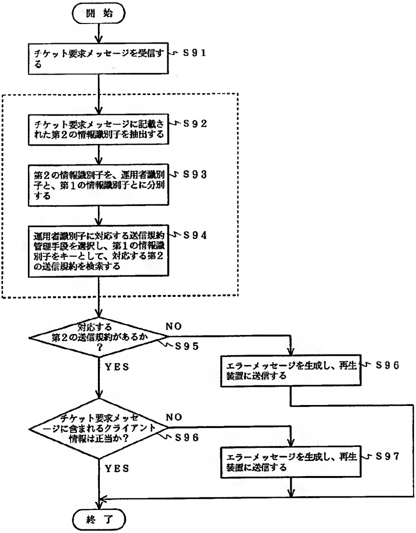
【図３０】


開　始
情報抽出完了メッセージを受信する
S111
セッション鍵要求メッセージを生成し、第２のストリーミングサーバ装置へ送信する
S112
終　了

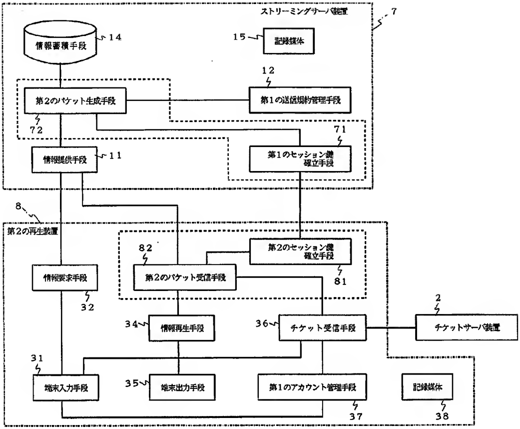
【図３１】


開　始
セッション鍵要求メッセージを受信する
S121
乱数を生成し、一時記憶する
S122
乱数を第２の再生装置へ送信する
S123
終　了

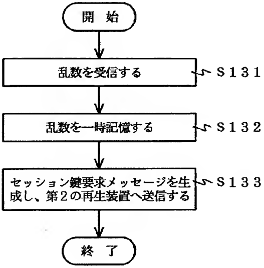
【図２４】


開 始
チケット要求メッセージを受信する
S91
チケット要求メッセージに記載された第２の情報識別子を抽出する
S92
第２の情報識別子を、運用者識別子と、第１の情報識別子とに分別する
S93
運用者識別子に対応する送信規約管理手段を選択し、第１の情報識別子をキーとして、対応する第２の送信規約を検索する
S94
対応する第２の送信規約があるか？
S95
NO
YES
エラーメッセージを生成し、再生装置に送信する
S96
チケット要求メッセージに含まれるクライアント情報は正当か？
S96
NO
YES
エラーメッセージを生成し、再生装置に送信する
S97
終 了

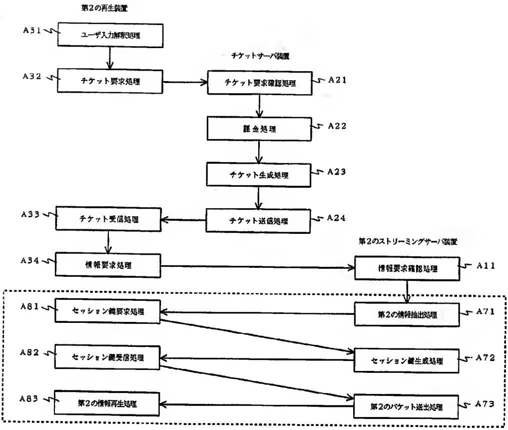
【図27】


ストリーミングサーバ装置
7
情報蓄積手段
14
15
記録媒体
12
第2のパケット生成手段
第1の送信規約管理手段
72
71
情報提供手段
11
第1のセッション鍵確立手段
8
第2の再生装置
82
第2のセッション鍵確立手段
情報要求手段
第2のパケット受信手段
81
32
2
34
情報再生手段
36
チケット受信手段
チケットサーバ装置
31
端末入力手段
35
端末出力手段
第1のアカウント管理手段
記録媒体
37
38

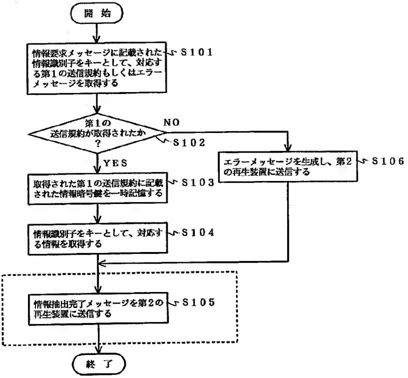
【図32】


開 始
乱数を受信する
S131
乱数を一時記憶する
S132
セッション鍵要求メッセージを生成し、第2の再生装置へ送信する
S133
終 了

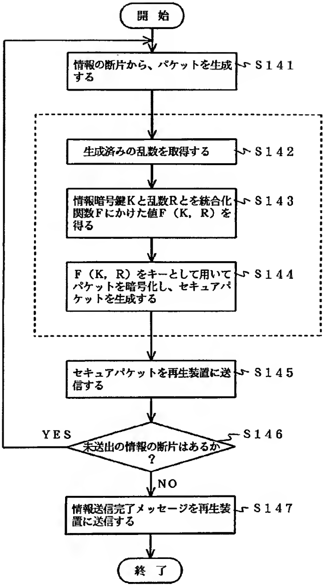
【図２８】


第2の再生装置
A31
ユーザ入力解釈処理
A32
チケット要求処理
チケットサーバ装置
チケット要求確認処理
A21
課金処理
A22
チケット生成処理
A23
A33
チケット受信処理
チケット送信処理
A24
第2のストリーミングサーバ装置
A34
情報要求処理
情報要求確認処理
A11
A81
セッション鍵要求処理
第2の情報抽出処理
A71
A82
セッション鍵受信処理
セッション鍵生成処理
A72
A83
第2の情報再生処理
第2のパケット送出処理
A73

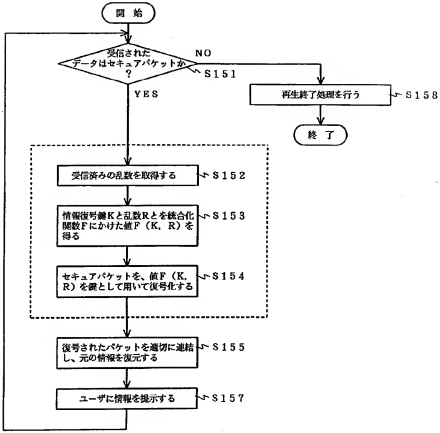
【図２９】


開 始
情報要求メッセージに記載された情報識別子をキーとして、対応する第１の送信規約もしくはエラーメッセージを取得する
S101
第１の送信規約が取得されたか？
NO
S102
YES
取得された第１の送信規約に記載された情報暗号鍵を一時記憶する
S103
エラーメッセージを生成し、第２の再生装置に送信する
S106
情報識別子をキーとして、対応する情報を取得する
S104
情報抽出完了メッセージを第２の再生装置に送信する
S105
終 了

【図３３】


開 始
情報の断片から、パケットを生成する
S141
生成済みの乱数を取得する
S142
情報暗号鍵Kと乱数Rとを統合化関数Fにかけた値F（K，R）を得る
S143
F（K，R）をキーとして用いてパケットを暗号化し、セキュアパケットを生成する
S144
セキュアパケットを再生装置に送信する
S145
未送出の情報の断片はあるか？
S146
YES
NO
情報送信完了メッセージを再生装置に送信する
S147
終 了

【図３４】



フロントページの続き

(51) Int.Cl.⁷		識別記号	F I		テーマコード（参考）
Ｈ０４Ｌ	9/08		Ｈ０４Ｎ	7/173	６１０Ｚ
	9/32			7/167	Ｚ
Ｈ０４Ｎ	7/167		Ｈ０４Ｌ	9/00	６０１Ｂ
	7/173	６１０			６７３Ａ

Ｆターム（参考）　5C064 BA07 BB01 BB02 BC04 BC06
BC17 BC18 BC22 BC23 BD02
BD08 BD09 CA14 CB01 CC01
CC04
5J104 AA01 AA07 AA16 EA01 EA04
KA01 NA02 PA07 PA11